Technical Documentation

This PDF was generated for mobilEcho 4.1.

For the latest version of our technical documentation, please see http://docs.grouplogic.com.

For questions, please email support@gropulogic.com.

GroupLogic®

MobilEcho Home

Welcome to mobilEcho 4.2

Select the document that you require.

- mobilEcho Quick Start Guide - Takes you through the essential steps for installing mobilEcho Server and setting up your first shared volume.
- mobilEcho Server User Manual - Contains full details on configuring and using mobilEcho File Server and mobilEcho Client Management Server.
- mobilEcho Client Application User Guide - Contains full details on installing and using the mobilEcho client application.

A PDF version of this documentation can be downloaded from here.

If you'd like to export the whole documentation or just specific pages, you can do so from this page, or by going to **Browse** -> **Advanced** -> **PDF Export**.

mobilEcho Quick Start Guide

Welcome to mobilEcho

This guide provides the essential steps for setting up a **mobilEcho File Server**. For more detailed instructions on configuring the mobilEcho File Server and the optional **mobilEcho Client Management Server** component, see the relevant sections of the complete user manual:

- mobilEcho File Server
- mobilEcho Client Management Server

Before you begin

Verify that your server meets the following requirements.

Operating System Requirements

Windows Server Platforms: 2012, 2008 (inc. R2), 2003 (inc R2)

Windows Workstation Platforms: Windows 7, Vista, XP Pro SP3

Minimum Hardware Recommendation

Processor: Pentium 4

Memory: 1 GB

Network Requirements

mobilEcho clients require network access to your server.

If you want to allow access from outside your firewall, there are several options:

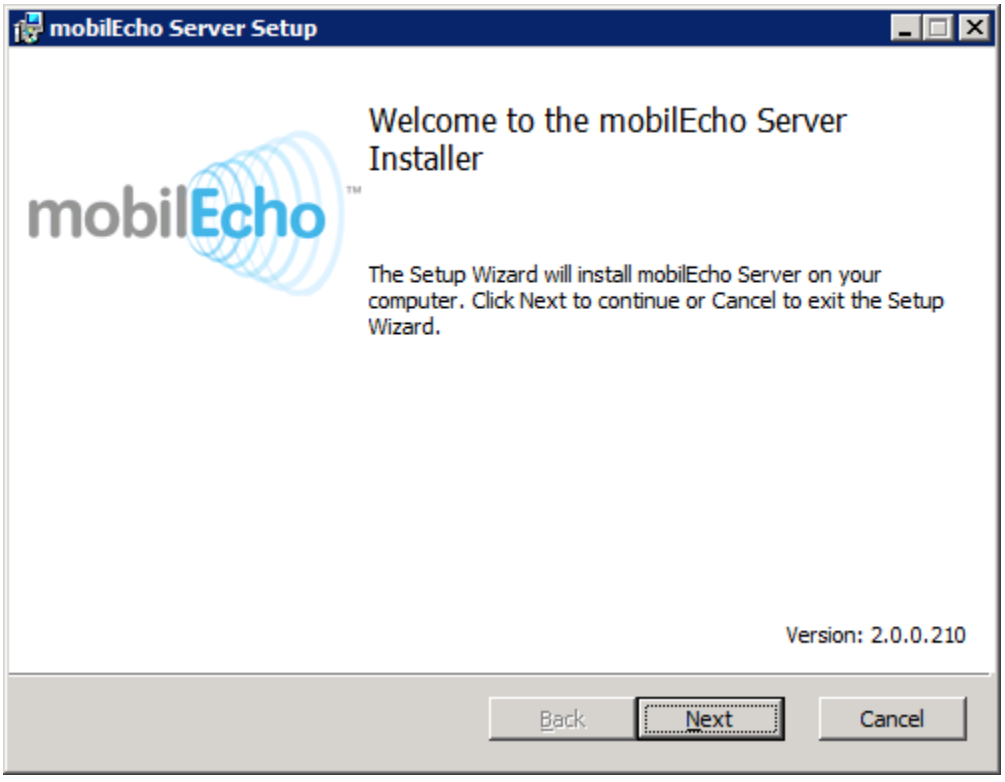
- Port 443 access
- VPN connection
- Reverse proxy server

See the Getting Started section of the mobilEcho Server User Manual for further details on this access options.

Installing MobilEcho on your server

1. Run the **mobilEcho Installer**. Be sure you are logged into Windows with administrator privileges.

2. Click **Next** to begin installation.



3. Accept the Software License Agreement and click **Next**.

4. Click **Next** to accept the default Destination Folder.

5. Click **Install** to begin the installation.

> **Upgrade installs**
>
> If you have a previous version of mobilEcho installed, it will be upgraded to the new version. Any existing settings will be retained.

6. Click **Finish** to close the completed installer and automatically launch the mobilEcho Administrator.

First run - Installing your license

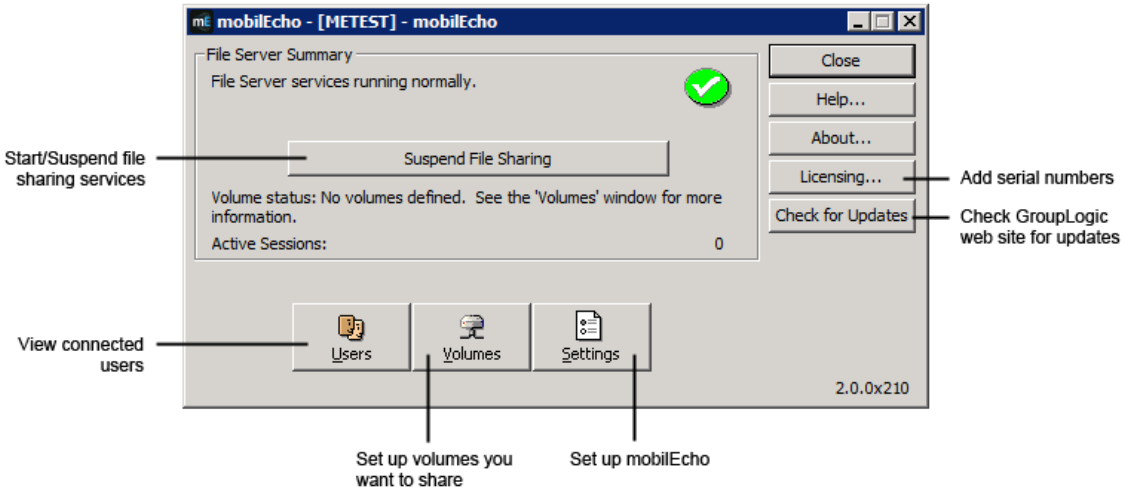
If you are installing mobilEcho for the first time, mobilEcho will ask if you would like to replicate your existing Windows SMB file shares or ExtremeZ-IP AFP file volumes. No data is copied or changed. The corresponding share locations are simply added as volumes in mobilEcho. This can also be done at any time from within the mobilEcho Volumes window.

New mobilEcho installations default to trial mode. If you have a mobilEcho serial number, click **Licensing** and then click **Add License** to add your serial number.

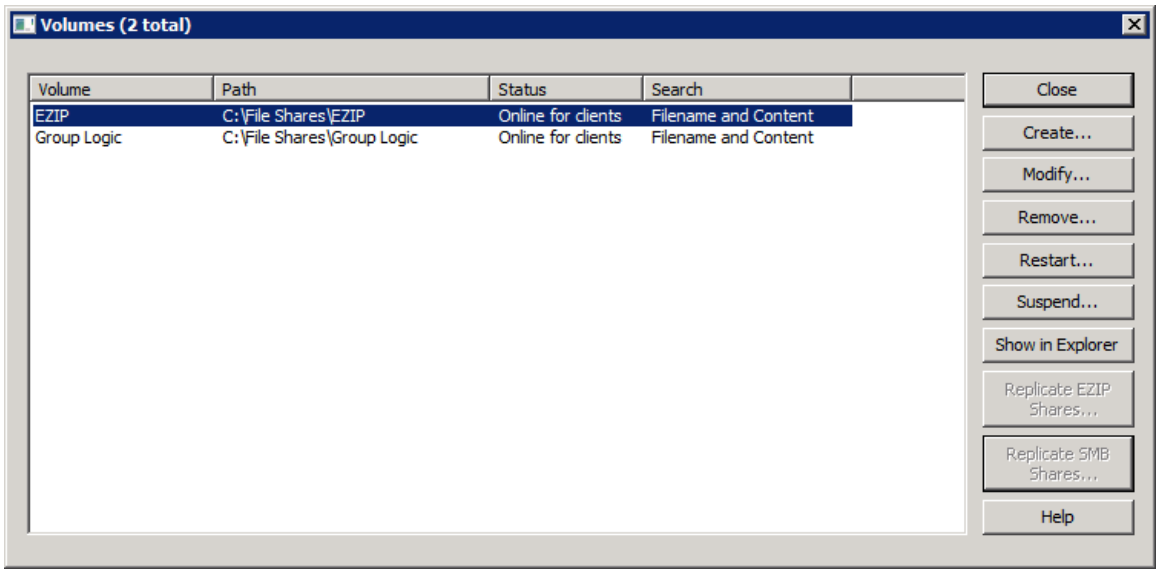
If you upgraded a previous version of mobilEcho, it will continue to use your existing serial number.

Configuring your first shared volume

1. Launch the mobilEcho Administrator.

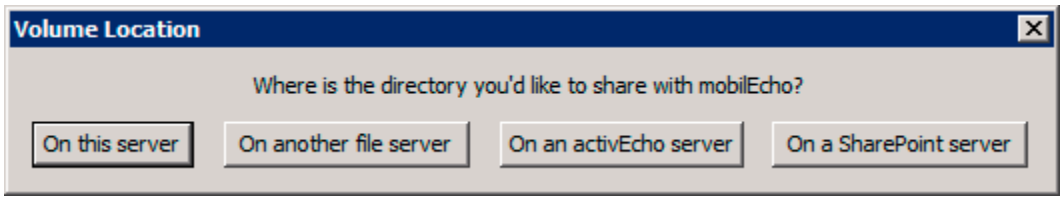


2. Click **Volumes**. The Volumes window will appear.

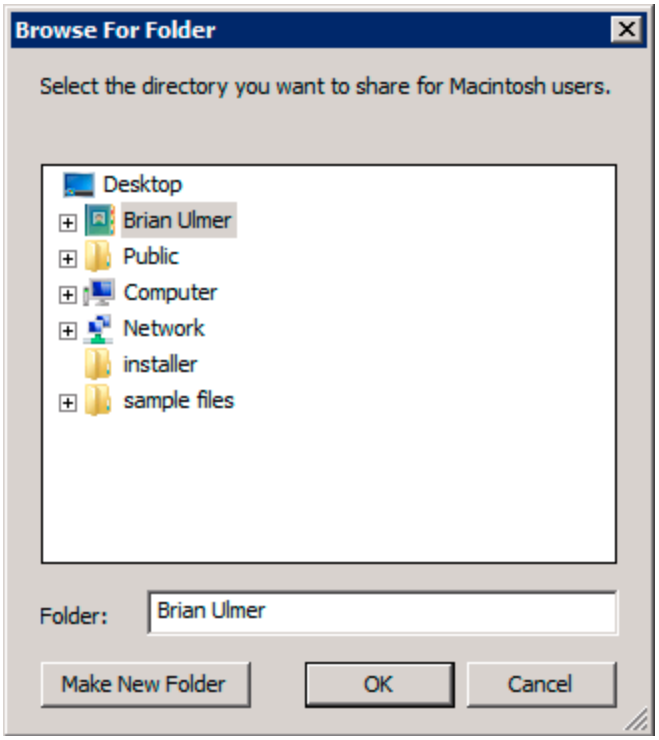


3. Click **Create** to create a new volume.

If you want to share files on this server's physical storage, choose **On this server**. If you want to share an SMB/CIFS volume located on another server or NAS device, choose **On another server**. If you want to give users access to your activEcho server, choose **On an activEcho server**. If you want to give access to a SharePoint server, choose **On a SharePoint server**. The ability to create mobilEcho volumes that give access to SMB/CIFS shares and SharePoint servers requires a mobilEcho enterprise or trial license. The ability to share an activEcho server is derived from the activEcho license. If you own a "standalone" mobilEcho server license, you will only see the options to share locations **On this server** and **On an activEcho server**.

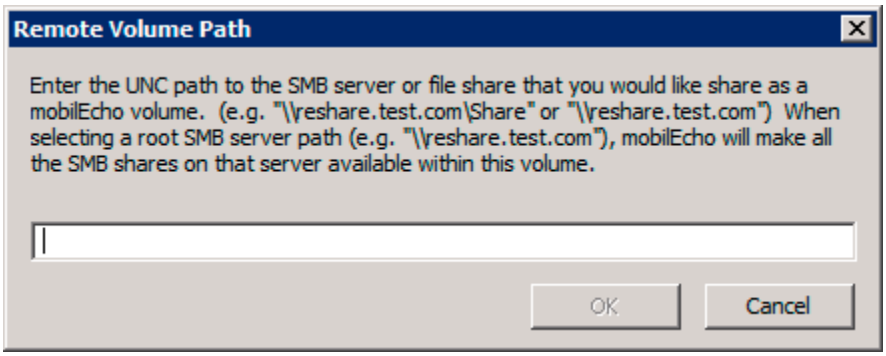


If you choose **On this server**, or if you are running a mobilEcho Server with a perpetual license (which does not support resharing volumes on other servers), you will be prompted to select a directory location on this server. Browse to the path of the folder you want to share and click **OK**.



If you choose **On another server**, you will be prompted to enter the path to the server or SMB share you'd like to make available with this mobilEcho volume. Enter the desired path and click **OK**.

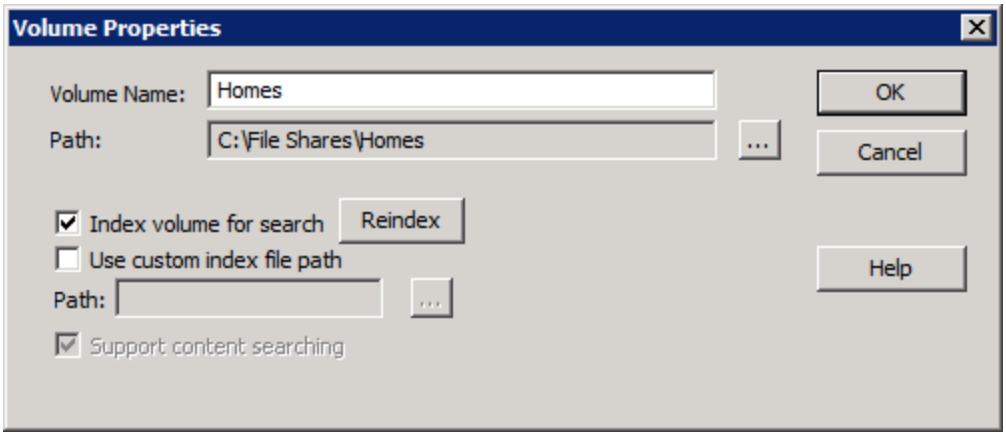
> **Microsoft Distributed File System (DFS) namespaces**
>
> mobilEcho's network reshare feature can be used to make DFS namespaces available to mobilEcho users. Simply specify the DFS namespace's path when creating an **On another server** volume.



Details on configuring activEcho volumes can be found here.

Details on configuring SharePoint volumes can be found here.

4. The Volume Properties dialog appears. Edit the **Volume Name** if necessary.



5. Click **OK** to share the volume with mobilEcho.

Installing the mobilEcho client application

1. Browse to mobilEcho in the Apple or Android app store:

   From your iOS device, visit the Apple App Store and search for mobilEcho, or follow this link:

   - http://www.grouplogic.com/web/meappstore

   From your Android device, visit the Google Play store and search for mobilEcho, or follow this link:

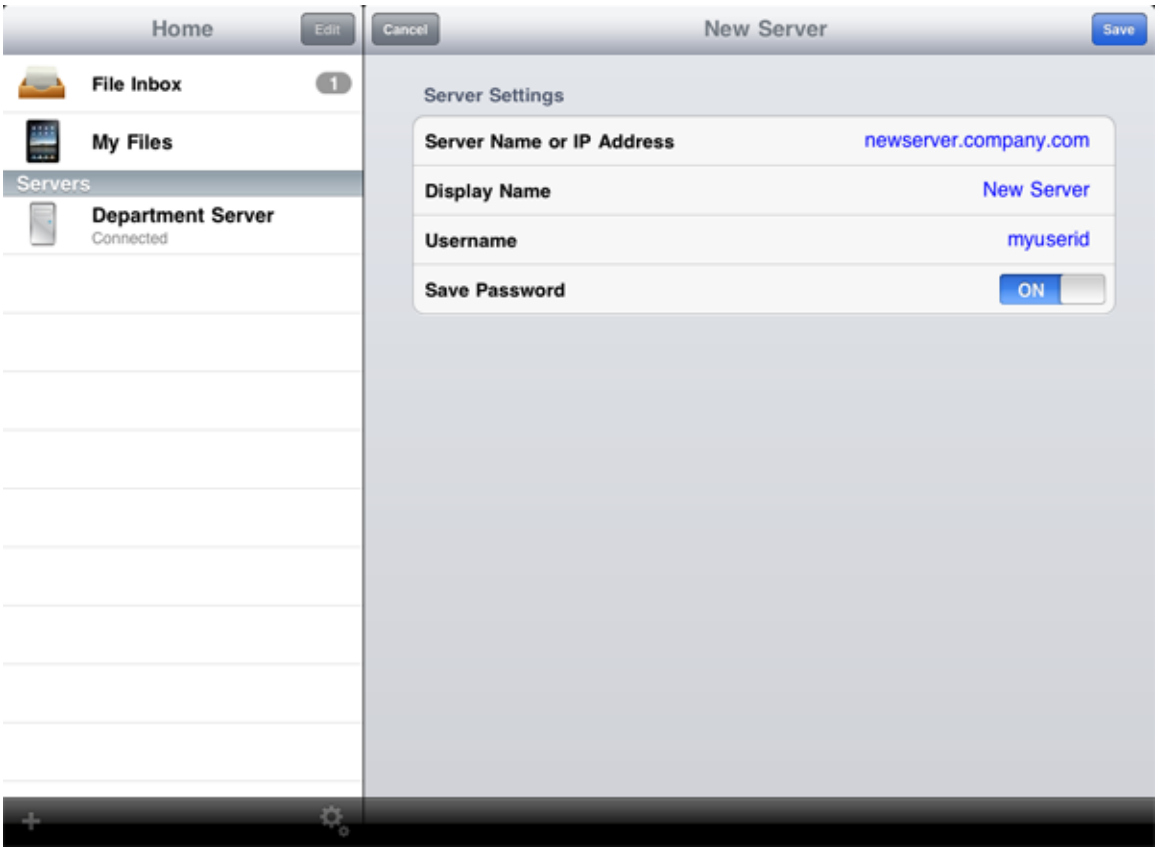
   - https://play.google.com/store/apps/details?id=com.grouplogic.mobilecho

2. Install the mobilEcho app and tap it to launch mobilEcho.

3. At the Welcome screen, tap **Continue**.

4. Tap the "**+**" icon on iOS to add a server. On Android, open the Settings menu and tap "**Add Server**".

5. Enter the **Server Name or IP address** of the server you installed mobilEcho on. You can optionally enter a **Display Name** for this server, which will appear in the mobilEcho server list.

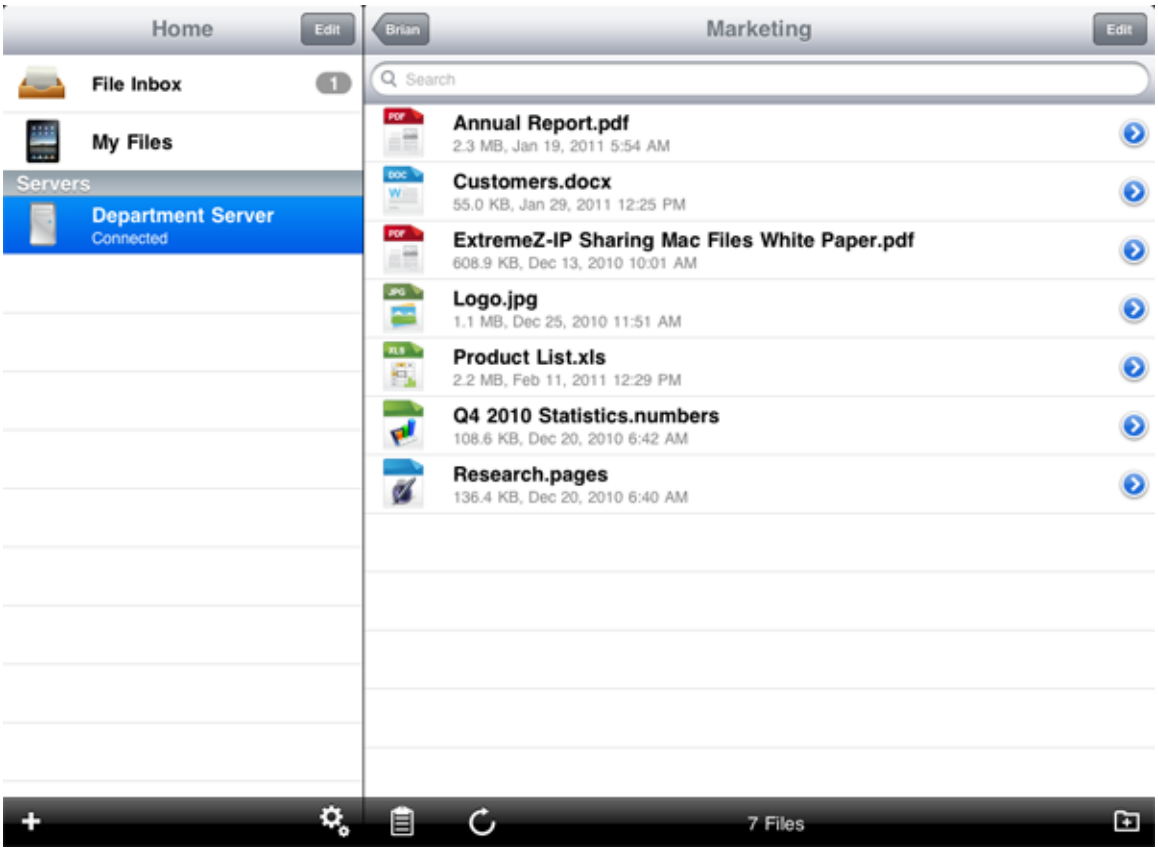


6. Enter a **Username** that has access to the mobilEcho file server. mobilEcho uses standard NTFS permissions to regulate access.

7. Toggle **Save Password** to **ON** if you would like to save your password, then enter and confirm your password.

8. Tap **Save** to commit the server settings.

9. Tap the server listed in the left hand pane to connect and browse available volumes.



For full details on the mobilEcho client application's settings and features, visit the mobilEcho Client Application User Guide page.

> **Windows 2003 Service Dependencies**
>
> mobilEcho uses Windows' embedded web services for HTTPS communications. While this does not require you have the Internet Information Server (IIS) role active on your Windows 2003 server, mobilEcho is dependent on two related Windows services: **IIS Admin Service** and **HTTP SSL**. After installation, if mobilEcho clients are unable to connect to your server, ensure that these two Windows services are enabled and running.

Additional resources

GroupLogic Support web site

MobilEcho documentation site

Search the Knowledge Base

Submit a support request

mobilEcho Server User Manual

Welcome to mobilEcho. Please select a topic below.

Getting Started

Introduction

mobilEcho is the industry's first and only mobile file management (MFM) software for enterprise iPad and iPhone users. mobilEcho enables enterprises to provide mobile device users with secure access to enterprise file servers, eliminating the need for work-arounds and third-party mobile applications that compromise the security of enterprise files and assets.

mobilEcho Server includes two components:

- **mobilEcho File Server**
- **mobilEcho Client Management Server**

mobilEcho Server must be installed on at least one server on your network. mobilEcho servers are able to give mobile clients access to files stored directly on the server where mobilEcho is installed, or to proxy access to files on other servers or NAS devices on your network that support the standard SMB/CIFS protocol. The **mobilEcho File Server** component handles core file server functionality and is required for mobile file access.

The **mobilEcho Client Management Server** component is installed with mobilEcho Server, but is disabled by default. **mobilEcho Client Management** provides comprehensive tools to allow administrators to set policies and permissions for mobile devices that access their mobilEcho servers. These tools ensure IT has full control over mobile device access to corporate files. **mobilEcho Client Management** allows profiles to be assigned to Active Directory users or groups. Typical deployments need only one mobilEcho server to act as the **mobilEcho Client Management Server**.

System Requirements

mobilEcho Server can be installed on both server and workstation-class versions of the Windows operating system. For optimal results, your Windows machine should be running the latest service pack from Microsoft.

Windows System Requirements

- Windows server platforms: 2012, 2008 (inc. R2), 2003 (inc. R2)
- Windows workstation platforms: Windows 7, Vista, XP Pro SP3

Minimum Hardware Requirements

- Processor: Pentium 4
- Memory: 1 GB

Network Requirements

mobilEcho ensures that all data transfer is secure between the server and the client. All mobilEcho traffic is sent end-to-end as encrypted HTTPS. It doesn't matter whether your user is accessing a file server from the office, over 3G or from a public Wi-Fi hotspot. The data is always encrypted and secure.

If you want to allow access from outside your firewall, there are several options:

1. **Port 443 access:** mobilEcho uses HTTPS for encrypted transport, so it fits in naturally with common firewall rules allowing HTTPS traffic on port 443. If you allow port 443 access to your mobilEcho server, authorized iPad clients can connect while inside or outside of your firewall. mobilEcho can also be configured to use any other port you prefer.
2. **VPN:** mobilEcho supports access through a VPN connection. Both the built in iOS VPN client and third-party VPN clients are supported. iOS management profiles can optionally be applied to devices using Mobile Device Management (MDM) systems or the Apple iPhone Configuration Utility to configure the certificate-based iOS "VPN-on-demand" feature, giving seamless access to mobilEcho servers and other corporate resources.
3. **Reverse proxy server:** If you have a reverse proxy server set up, iPad clients can connect without the need for an open firewall port or a VPN connection. The mobilEcho client app supports reverse proxy pass-through authentication, username / password authentication, and certificate authentication. For details on adding certificates to the mobilEcho client app, click here .
4. **Good Dynamics enabled mobilEcho client app:** The mobilEcho client app includes the ability to be enrolled in and managed by the Good Dynamics platform. In this configuration, all network communication between mobilEcho clients and mobilEcho servers is routed through the Good Dynamics secure communication channel and Good Proxy Server. For more details, see the mobilEcho for Good Dynamics manual page.

The mobilEcho Client Management system also has the ability to configure the client application to only allow connections to servers with valid X.509 SSL certificates.

mobilEcho Topology

mobilEcho clients connect directly to your server rather than utilizing a third-party service, leaving you in control. mobilEcho server can be installed on existing file servers, allowing iPads and iPhones access files located on that server. These are typically the same files already available to PCs using Windows file sharing and Macs using ExtremeZ-IP File Server.

Clients access mobilEcho servers using their Active Directory user account. No additional accounts need to be configured within mobilEcho. mobilEcho also supports file access using local computer accounts

configured on the Windows server mobilEcho is running on, in the event you need to give access to non-AD users. The **mobilEcho Client Management** features described below require AD user accounts.

A minimal mobilEcho deployment consists of a single Windows server running a default installation of mobilEcho. This default installation includes the **mobilEcho File Server** component enabled and the **mobilEcho Client Management Server** component installed, but disabled. This scenario allows devices running the mobilEcho client application to connect to this single file server, and leaves the configuration of client app settings and configuration of the servers the client will connect to, up to the iPad or iPhone user.

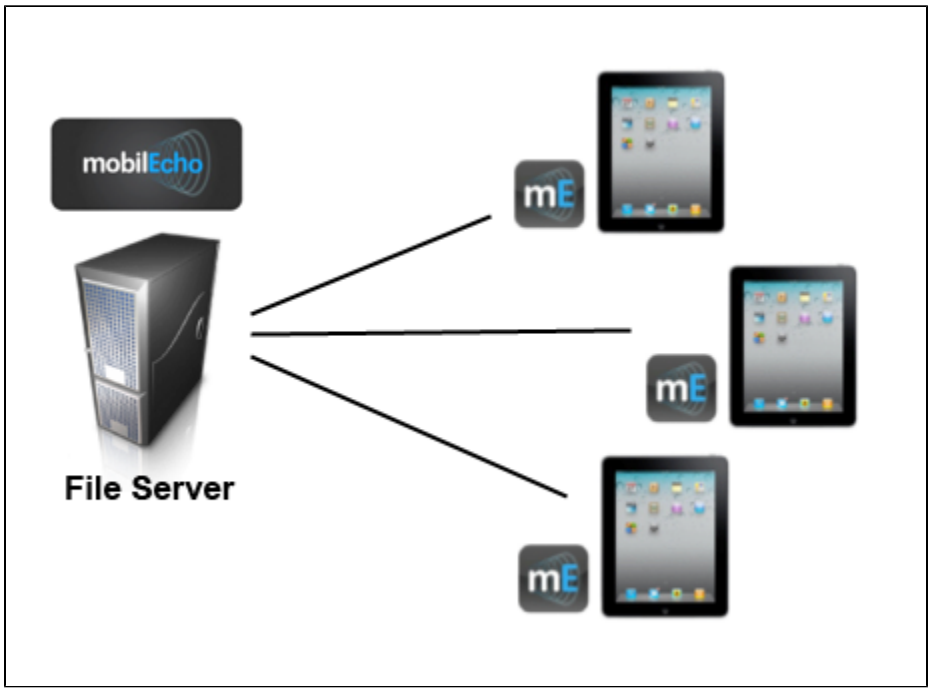


Fig 1. Single mobilEcho File Server, many mobilEcho clients

Any number of mobilEcho servers can later be added to the network and configured for access from the mobilEcho client app.

mobilEcho servers also have the ability to make files located on other servers available to mobile clients. By using mobilEcho's **Network Reshare** feature, shared volumes can be created on a mobilEcho server that point to a remote SMB/CIFS file share. This feature allows access to multiple servers to be provided through a single mobilEcho server. The **Network Reshare** feature is included with annual subscription Enterprise License Program (ELP) licenses.

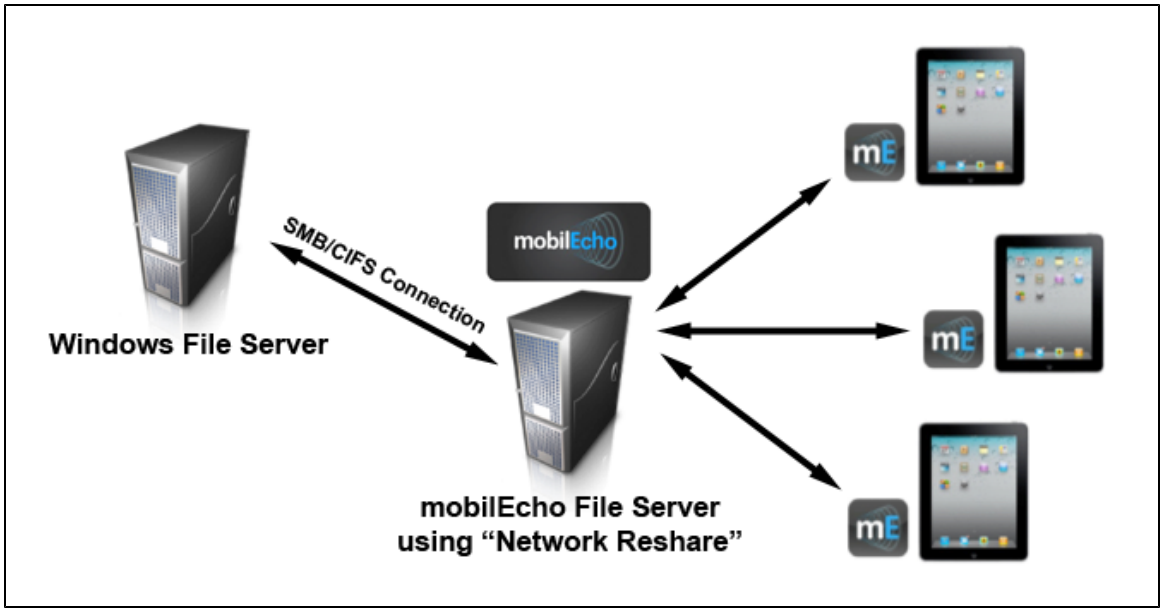


Fig 2. Single mobilEcho File Server, also making remote files available using Network Reshare

Details on installing mobilEcho Server are included in the Installation section of this guide. Configuration of shared volumes and server settings are covered in the mobilEcho File Server section.

mobilEcho Client Management Server

If you wish to remotely manage your mobilEcho clients, a mobilEcho Server must have its **mobilEcho Client Management Server** component enabled. Client management allows you to create profiles per Active Directory user or group. These profiles can:

- Configure general application settings
- Assign servers, folders, and home directories to be displayed in the mobilEcho client
- Restrict what can be done with files
- Restrict the other third party apps that mobilEcho files can be opened into
- Set security requirements (server login frequency, application lock password, etc.)
- Disable the ability to store files on the device
- Disable the ability to include mobilEcho files in iTunes backups
- Remotely reset a user's application lock password
- Perform a remote wipe of the mobilEcho client app's local data and settings
- And many additional configuration and security options

On a typical network, only one **mobilEcho Client Management Server** is required. This server can perform the **mobilEcho File Server** and **mobilEcho Client Management Server** roles simultaneously.

A typical network employing client management might include one server with the **mobilEcho File Server** and **mobilEcho Client Management Server** components enabled, and several additional mobilEcho servers acting only as **mobilEcho File Servers**. In this scenario, all mobilEcho iPad clients are configured to be managed by the designated management server, and will contact this server each time the mobilEcho application is started, to check for any changed settings and to accept application lock password resets and remote wipe commands if necessary.

mobilEcho clients can be assigned a list of servers, specific folders within shared volumes, and home directories in their management profile. These resources will automatically appear in the mobilEcho app and the client app will contact these servers directly as needed for file access.

Details on enabling and configuring the mobilEcho Client Management Server are included in the mobilEcho Client Management Server section of this guide.

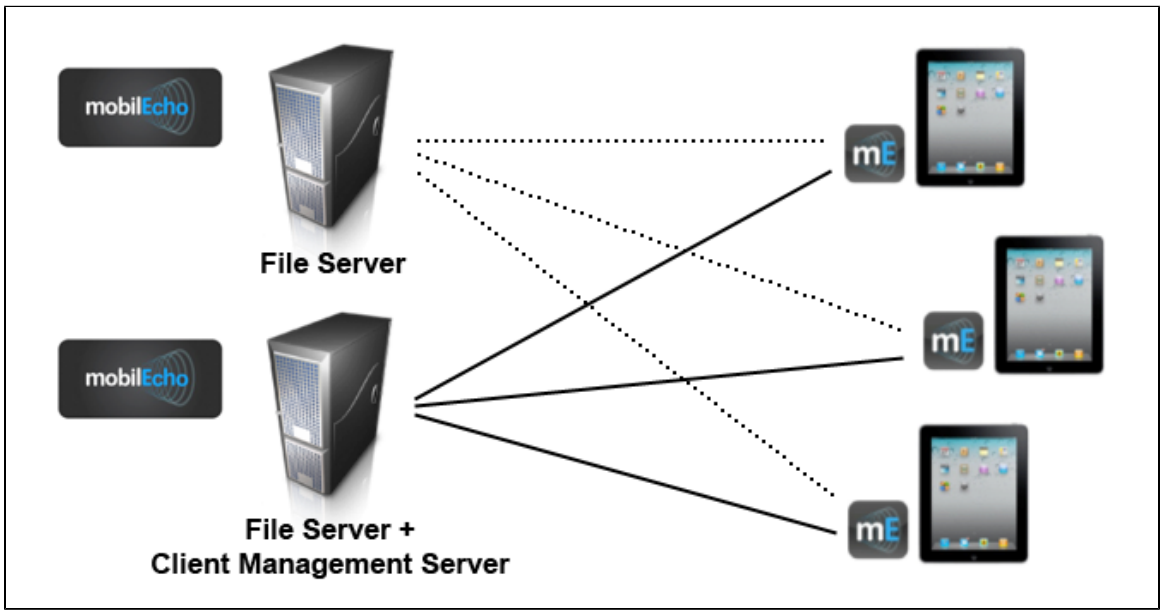


Fig 3. One mobilEcho File Server, one File Server + Client Management Server, many clients

Getting Help

In addition to this mobilEcho Server User Manual, GroupLogic offers several other sources of help.

You can visit GroupLogic at: http://www.grouplogic.com

You can find the latest release of mobilEcho at: http://support.grouplogic.com/?page_id=34

You can search the GroupLogic Knowledge Base at: http://www.grouplogic.com/knowledge

For the first year you own mobilEcho, technical support and upgrades are included in the price of the product. After your first year of free support, you can purchase extended support. For technical support services, submit a support request at http://www.grouplogic.com/support/requestform/ or call 1.703.528.1555, Monday through Friday, 8:00 am to 6:00 pm EST. Have your mobilEcho serial number ready for verification. In addition, you can send your questions to: support@grouplogic.com

The Maintenance and Support program includes important benefits -- e-mail and telephone technical support services for problems that you encounter, upgrades, bug fixes, and other incremental releases of the software.

Installation

Installing mobilEcho Server

The primary component of mobilEcho is a Windows Service that provides file sharing to mobile clients. This mobilEcho File Server includes an administrative tool, the mobilEcho Administrator, used to configure shared volumes and other settings.

The number of clients who can connect using mobilEcho depends on your license and its user count. You can upgrade your user count as necessary. mobilEcho counts each connected named user account as one user for licensing purposes. Each user account can connect from up to 3 unique devices. Each additional unique device is counted as an additional user.

If you are installing mobilEcho on a cluster. Please refer to the Installing on a Cluster section of this document.

Before Installing mobilEcho

The topics covered in this section give you information you need before installing mobilEcho.

Required Windows File Permissions for Shared Volumes

mobilEcho relies on the SYSTEM account on the Windows server to perform many of its core functions. For this reason, any folder hierarchy that is shared as a volume with mobilEcho requires that the SYSTEM account have Full Control access to the entire folder hierarchy. These permissions are the default for the Windows OS partition, but any additional disks or partitions containing mobilEcho volumes must have SYSTEM = “Full Control” set to allow mobilEcho to function properly. Please verify that all the volumes you share have this permission set.

Sharing the Root of a Drive

Although mobilEcho supports sharing out the root of the drive, Windows treats permissions at the root of the file system differently from other folders. We recommend that you do not share out drive letters directly. Instead, you should create a sub-folder for your shared volume.

Client-side file permissions & browsing of inaccessible items

When a mobilEcho client connects to a mobilEcho server and browses the contents of mobilEcho shared volumes, they do so in the context of their own user account. All permissions to read, modify, and delete files are determined by the NTFS permissions that their user account possesses for the files being accessed. If a user does not have read permissions for a particular shared volume, folder, or file, these items are filtered out and will not appear in the mobilEcho client.

Installing the mobilEcho Server Software

To install the mobilEcho server software, do the following:

1. Log into Windows with an administrator account.
2. Run the mobilEcho installer.
3. Follow the steps displayed by the installer. The only user-configurable option in the installer is the program installation location.

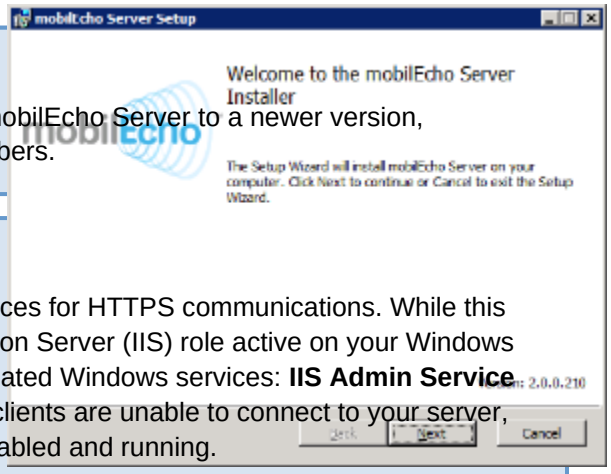
See the mobilEcho Quick Start Guide for detailed, step-by-step instructions.

Upgrading mobilEcho Server

If you are upgrading an existing installation of mobilEcho Server to a newer version, mobilEcho will retain all settings and serial numbers.

Windows 2003 Service Dependencies

mobilEcho uses Windows' embedded web services for HTTPS communications. While this does not require you have the Internet Information Server (IIS) role active on your Windows 2003 server, mobilEcho is dependent on two related Windows services: **IIS Admin Service** and **HTTP SSL**. After installation, if mobilEcho clients are unable to connect to your server, ensure that these two Windows services are enabled and running.

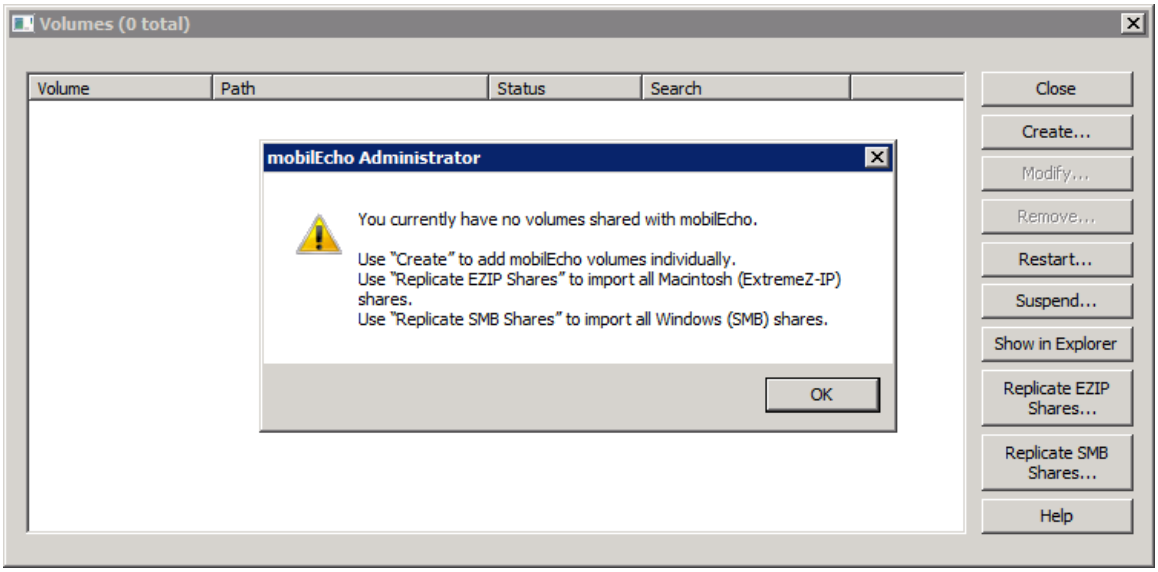


Launching mobilEcho Server the First Time

If you have the Windows firewall enabled and do not have a firewall exception for mobilEcho's default HTTPS port 443, mobilEcho will ask you if you'd like to add an exception automatically. If you choose not to, mobilEcho clients will not be able to connect to the server. An exception can be added or modified at any time through the Windows Firewall control panel.

When you launch the mobilEcho Administrator for the first time with no configured volumes (shares), mobilEcho prompts you to create new volumes or import existing volumes. mobilEcho can import existing volumes on your server that are shared using GroupLogic's ExtremeZ-IP File Server (AFP) and Windows file sharing (SMB).

During the import, mobilEcho configures mobilEcho volumes that correspond to the existing AFP or SMB shared volumes. No files are moved, modified, or duplicated. The same storage locations are simply shared as mobilEcho volumes. All existing Active Directory permissions continue to apply to mobilEcho users and regulate volume and file access in the same way they do for Mac and PC users.



> **Note:**
>
> You cannot create a volume with the name ***enroll***. This volume name is reserved for internal use.

Each subsequent time the mobilEcho Administrator is launched, mobilEcho checks for any EZIP or SMB shares that are not being shared as mobilEcho volumes. If any such shares exist, the **Replicate EZIP Shares** and/or **Replicate SMB Shares** buttons within the **Volumes** dialog become active. You can replicate newly added shares at any time by returning to the **Volumes** dialog.

Installing on a Cluster

Setting Up mobilEcho Clustering

Clustering provides fast failover and quick restart of the services provided by a failed server node. You set up a mobilEcho cluster using Microsoft Cluster Servers (MSCS) - specially linked servers running the Microsoft Cluster Service. If one server fails or is taken offline, the other server or servers in the cluster immediately take over the failed server's operations. Applications running on the cluster are always available. Resources running on multiple servers appear to connected clients as a single system, referred to as a mobilEcho virtual server. When a successful failover occurs because of a problem, the connected user sometimes cannot tell that service was interrupted.

mobilEcho is a cluster-aware application that you can use on active/active clustered configurations. Multiple instances of mobilEcho can run on a single server node. Each instance has its own IP address

and can be assigned its own shared volume. The configuration of multiple virtual servers provides server consolidation and load management benefits. Running multiple instances of mobilEcho on a server node provides high reliability because each instance runs in isolation from the others.

For help in configuring a cluster, see the following Cluster Worksheet. mobilEcho supports the following services in clustered configurations:

- active-active clustering
- multiple virtual servers per node in a cluster
- improved reliability and availability
- eight-node clusters in Windows Server 2003 & 2008
- possible server consolidation

When you are running mobilEcho in a clustered environment, the mobilEcho Administrator window shows the following in the title bar:

- the name of the server in upper case characters
- the name of the service in upper or lower case, as you typed it when you set up the service

MSCS uses the following terms to describe the component parts of a cluster configuration. Do not confuse these terms as you proceed with installing mobilEcho.

- **Node**---A single member server in a cluster.
- **Resource**---A hardware or software component that runs in a cluster, such as a disk, an IP address, a network name, or an instance of the mobilEcho service.
- **Group**---A combination of resources that are managed as a unit of failover. Groups are also known as resource groups or failover groups. A typical mobilEcho failover group consists of a disk, an IP address, a network name, and an instance of mobilEcho.
- **Dependency**---A service or other resource that must be available first in order for the dependent service to start.
- **Failover**---The process of moving resources or resource groups from one server to another. Failover can occur when one server experiences a failure of some sort or when you, the administrator, initiate the failover. This term is equivalent to Microsoft Cluster Administrator action of moving a Cluster Group to another node.
- **Quorum Resource**---A disk resource containing the failover information that is shared between nodes in a cluster.
- **Heartbeat**---The communication between Cluster nodes tells the other nodes that the service is still running.
- **Virtual Server**---A virtual server is a combination of configuration information and cluster resources, such as an IP address, network name and an application resource. A mobilEcho Virtual Server (MVS) is defined by its unique IP address.
- **Active/Active**---This term describes a configuration in which multiple nodes are mobilEcho file servers running in production.
- **Active/Passive**---This term describes a configuration in which one node is active in production and another node sits idle until a failover occurs.
- **Shared Storage**---This term refers to the external SCSI or fibre channel storage system. Shared storage is a requirement for multi-node clusters. Although this storage is shared, only one node can access an external storage resource at any given time.

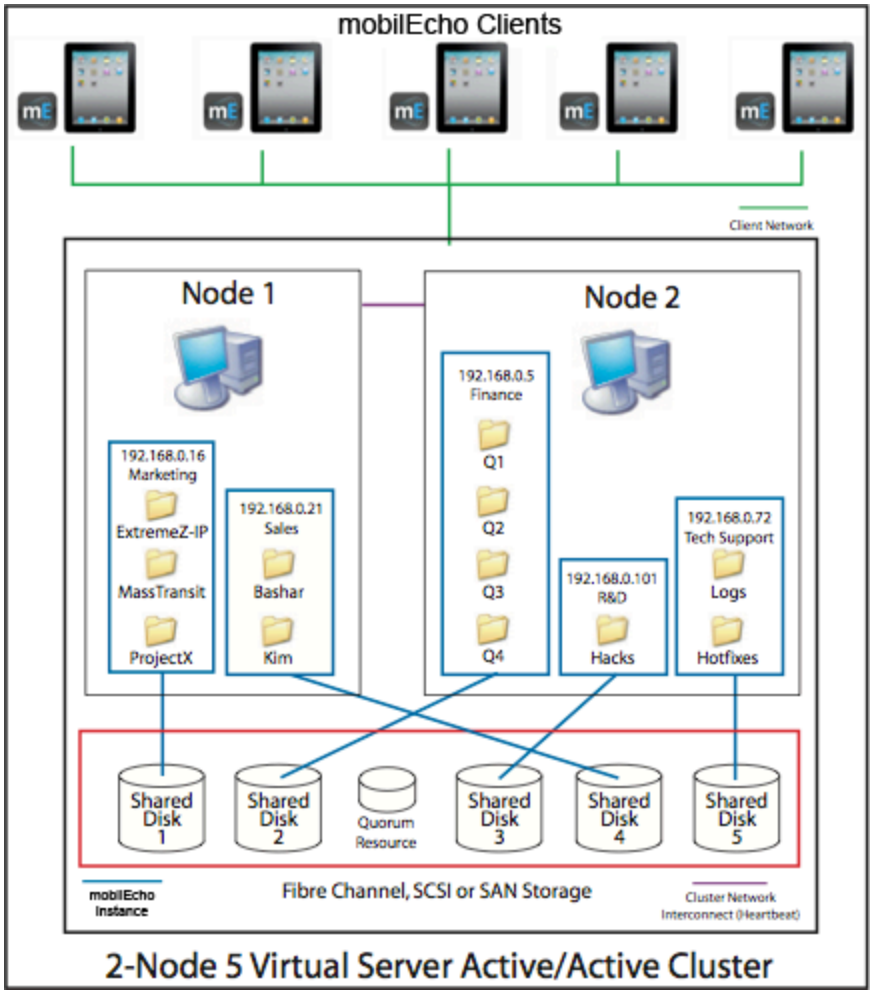


Fig 1. This diagram shows an example of a cluster setup.

> **NOTE**
>
> Each server has its own IP address. You can configure multiple shares for each virtual server.

Cluster Worksheet

For each mobilEcho service running on your cluster you will need the following:

1. A name for the unique mobilEcho service
2. A unique IP address and optionally a network name
3. Shared physical storage
4. A cluster group in which to put the new mobilEcho service

To simplify this process we have provided a worksheet to prepare for your installation. Duplicate the worksheet for each additional mobilEcho virtual server you would like to create.

INFORMATION NEEDED TO INSTALL THE SOFTWARE	
Serial Number:	

For each virtual server you want to set up, you will need to have unique values for all the sections below.

INFORMATION NEEDED TO CREATE A NEW SERVICE	
Unique service name	

INFORMATION NEEDED TO SET UP A NEW CLUSTER GROUP			
Cluster Group name			
IP address			
Network name (DNS/Netbios name)			
Unique service name (created above)			
Volumes to be shared	Drive Letter	Volume Name	Is the volume shared with Windows?

Installing mobilEcho on a Cluster

Before installing mobilEcho on a new cluster, you must have installed and configured the clustering service on your servers. On Windows 2003 Server (Enterprise, Storage Node Server, or Datacenter Edition) you will need to install and configure Microsoft Cluster Service. On Windows Server 2008 (Enterprise or Datacenter Edition), you will need to install and configure the Failover Clustering role. In addition, you need the following:

- A mobilEcho cluster-enabled serial number that is encoded with the number of nodes and virtual servers for which it is licensed. Use a single serial number for all the nodes of the cluster.
- A shared disk or disks where the mobilEcho shared volumes will reside.
- An IP address and network name for each mobilEcho virtual server you want to create; create a DNS entry for each IP address.

Reviewing the Installation Procedure

Installation consists of the following four parts, each with a number of steps that are described in the following sections:

1. Use the installer and serial number provided by Group Logic to install the mobilEcho on each node of the cluster.
2. Use the mobilEcho Administrator application to configure the necessary mobilEcho service(s) on each node of the cluster.
3. Use the Microsoft Cluster Administrator application, provided with Windows 2003, or the Failover Cluster Management application, provided with Windows Server 2008, to configure the Microsoft clustering service.
4. Use the mobilEcho Administrator application to configure shared folders and other features of the mobilEcho service.

Configuring mobilEcho Services

To operate, mobilEcho requires the following four components:

- IP Address
- Network Name
- Physical Disk
- mobilEcho Service

Place each set of components in its own cluster group or mobilEcho Virtual Server (MVS).

The number of MVSs created is based on the number of physical disks that need to be shared out with mobilEcho. For example, if the volumes are on three physical disks, create three MVSs. This configuration has the most flexibility; however, it requires you devote multiple IP addresses. If you create multiple MVSs, you can have multiple physical disks shared out by one MVS. The Cluster Worksheet in this guide can help you set up a plan for your cluster.

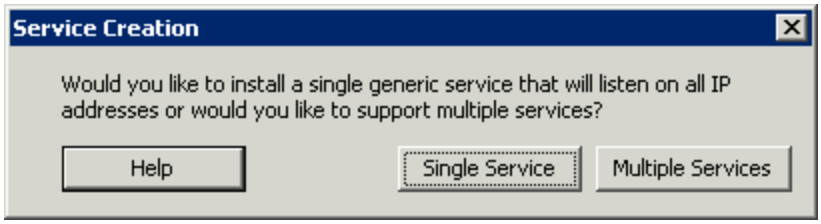
Creating a mobilEcho Service

Each mobilEcho virtual server you want to use requires a mobilEcho service instance. Each of these mobilEcho services requires a unique Service Name. When mobilEcho is installed on a cluster enabled server, no services are created by default. In this step, you will create a new mobilEcho service for each virtual server, on each node you want the service to run on.

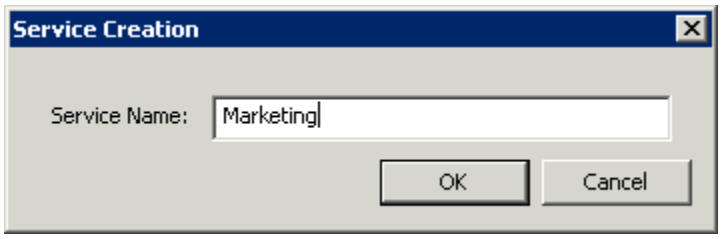
> **NOTE**
>
> Some illustrations below refer to GroupLogic's ExtremeZ-IP File Server product. mobilEcho uses the same cluster management system and the dialogs are the same, just referring to mobilEcho.

To create a mobilEcho service, do the following:

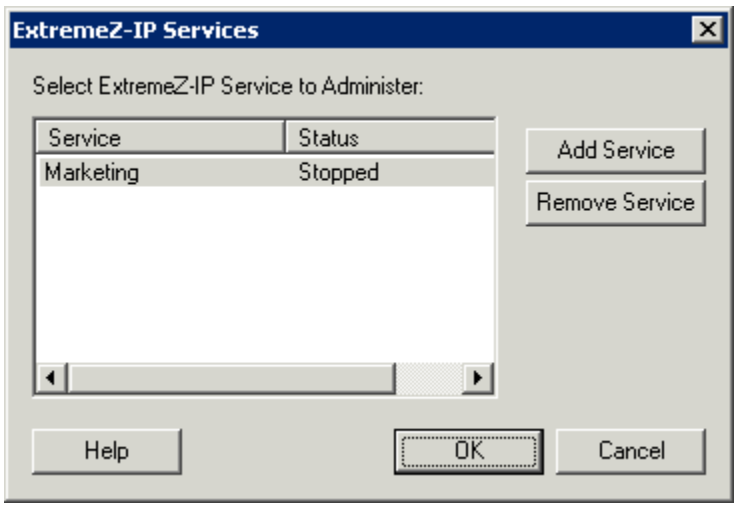
- After completing the mobilEcho installation process, or on a cluster server with an existing mobilEcho installation, run the **mobilEcho Administrator** application.
- If mobilEcho is being installed for the first time and no services exist, you will be prompted to create a service.
- When setting up a cluster, choose **Multiple Services**.



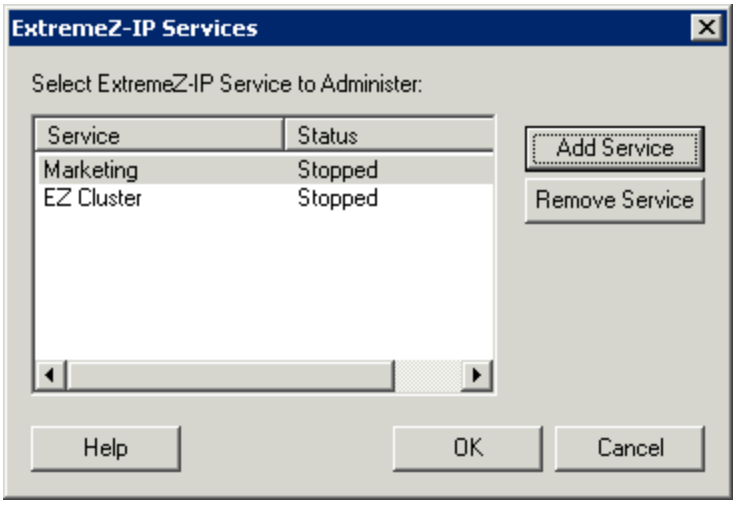
- You will be prompted to create your first service. Enter the **Service Name** of your choosing. In this example, our service name is “Marketing”. NOTE: Write down the exact service name you use in this command. You need the exact name when configuring Microsoft clustering in the next section.



- After the service is created, it will appear in the **mobilEcho Services** window. **mobilEcho Services** will be shown each time the **mobilEcho Administrator** is launched. It is used to select the service you would like to administer, as well as to add or remove additional services.



- If you are configuring multiple services, select **Add Service** and to create any additional services necessary.



- You will need to perform these steps on each cluster node that these mobilEcho services will run on.

Adding a mobilEcho Service to a Cluster

You can configure the cluster for mobilEcho in a number of ways:

- If you already have set up a Cluster Group, simply add mobilEcho as a generic service to your Cluster Group.
- If you do not have any existing cluster group, follow the steps in the sections below, which take you through the process of using the Cluster Application Wizard® to configure the cluster group.
- Or, you may use another method with which you are familiar.

If folders shared over SMB for Windows clients reside on the same physical disk as your mobilEcho volumes, you can add the mobilEcho service to an existing group.

Creating a Windows 2008 Cluster Group

For Windows 2003 instructions, see the next section.

This is the recommended method for creating a new cluster group that includes a mobilEcho service. If you already have a cluster group configured and would like to add mobilEcho to that group, right click the cluster group and select **Add Resource - Generic Service**. Then follow the steps below to select the desired mobilEcho service. This will bypass the cluster group network and storage configuration steps.

Creating the Cluster Group

1. Open **Failover Cluster Management** in **Administrative Tools** and select your cluster on the left pane.

2. Right click on the cluster name and select **Configure a Service or Application**. This will launch the **High Availability Wizard**. Click **Next**.

3. Select **Generic Service** and click **Next**.

4. You must now select the **mobilEcho File Access Server for Mobile Devices** service to add. You may see multiple entries for mobilEcho in the list. Each entry will display the mobilEcho service name as defined when the service was created. Select the entry that includes the specific mobilEcho service name you would like to configure and click **Next**.

5. Enter the network service name for your cluster group. This will define the DNS name that clients will use to connect to this cluster group. Select the **Networks** mobilEcho that this cluster group will use and define an IP address for the cluster group on each selected network.

6. Select the storage volume(s) you would like to make available to this cluster group and click **Next**. These should be the volumes that contain the directories to be shared with mobilEcho.

7. Click **Next** on the **Replicate Registry Settings** step. No changes are necessary.

8. Click **Next** on the **Confirmation** step.

Setting Cluster Resource Dependencies

To ensure that cluster services start-up in correct order, you must set resource dependencies for the IP Address, Network Name, and the Physical Disk.

To set resource dependencies for the IP Address, Network Name, and the Cluster Disk, do the following:

1. From **Failover Cluster Management**, under **Other Resources** for the cluster group, right click on the **mobilEcho File Access Server for Mobile Devices** resource.

2. Click **Properties**.

3. Select the **Dependencies** tab.

4. Add the **IP Address**, **Network Name**, and the **Cluster Disk** as dependencies.

5. Click **OK**.

Since the mobilEcho resource is created under the High Availability Wizard, all the nodes in the cluster are owners for the resource. If you do not want this configuration, you can change it before you bring the service online.

To change the owners for the resource, click the **Advanced Policies** tab and modify the **Possible Owners** accordingly.

Bringing the New Resource Online

At completion of this configuration, the mobilEcho resource may be offline. You can now bring the new resource online.

To bring the mobilEcho resource online, do the following:

1. Right click the **mobilEcho File Access Server for Mobile Devices** resource.

2. Select **Bring this resource online**.

Creating a Windows 2003 Cluster Group

The following steps are not the only way to create a new cluster group, but they are generally the fastest and most reliable.

Creating the Cluster Group

1. Launch **Cluster Administrator**.

2. Right click on **Groups** and select **Configure Application**.

3. Click **Next** to begin the wizard.

4. Select Create a new virtual server and click **Next**.

5. Select **Create a new resource group** and click **Next**.

6. Enter a **Group Name**. Click **Next**.

7. Enter a **Network Name** and an **IP Address**. Click **Next**.

8. Click **Next** on the **Advanced properties for the new virtual server** dialog.

9. Select **Create a cluster resource for my application now** and click **Next**.

10. Select **Generic Service** as the **Resource Type**. Click **Next**.

> **Resource Type Selection**
>
> Make sure you select Generic Service. Selecting Generic Application, which is the default entry, is a common mistake.

11. Enter the **Resource Name** in the **Name** field. Use a functionally meaningful name to that the service is easy to identify. Click **Next**.

12. Enter the **Service name** with no **Start parameters**. This name must match the **Service name** configu red in the **mobilEcho Administrator Services** dialog. Click **Next**.

13. Click **Next** on the **registry replication** dialog. Then, click **Finish**.

To add a disk resource to the newly created group, do the following:

1. Right click on the group and select **New** > **Resource**. Then, select **Physical Disk** in the **Resource Type** drop-down list.

2. Click **Next**.

3. Configure the owners of the **Physical Disk** resource to be all of the nodes mobilEcho will run under. You can add dependencies for the Physical Disk, if needed, but this configuration is not required for mobilEcho.

4. Select the **Physical Disk** containing the folders you want to share with mobilEcho, and click **Finish**.

Setting Cluster Service Dependencies

To ensure that cluster services start-up in correct order, you must set resource dependencies for the IP Address, Network Name, and the Physical Disk.

To set resource dependencies for the IP Address, Network Name, and the Physical Disk, do the following:

1. From the **Cluster Administrator**, right click on the **mobilEcho service resource**.

2. Click **Properties**.

3. Select the **Dependencies** tab.

4. Click **Modify**.

5. Add the **IP Address**, **Network Name**, and the **Physical Disk** as dependencies.

6. Click **OK**.

Since the mobilEcho resource is created under the virtual server wizard, all the nodes in the cluster are owners for the resource. If you do not want this configuration, you can change it before you bring the service online.

To change the owners for the resource, click the **General** tab and modify the **Possible Owners** according ly.

Bringing the New Service Online

When you have configured MSCS on all nodes of the cluster for each Cluster Group that contains mobilEcho, MSCS setup is complete. Once you have configured your setup, you can bring the new service online.

To bring the Cluster Group online, do the following:

1. Right click the **Group**.

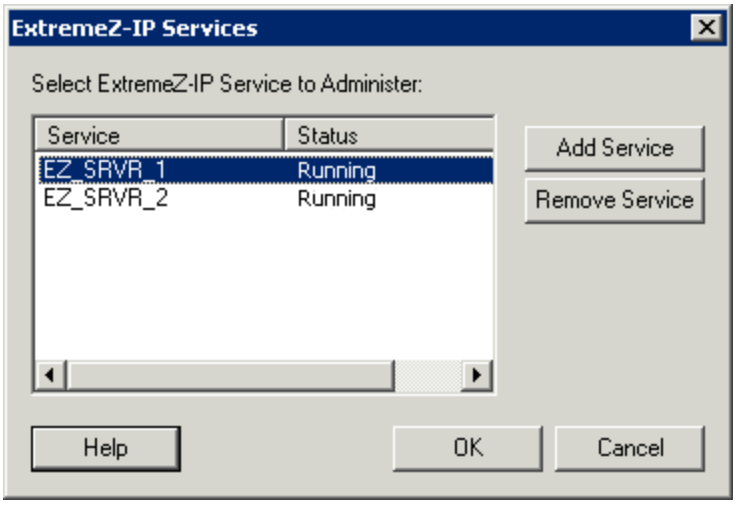
2. Select **Bring Online**.

Administering mobilEcho on a Cluster

In a clustered environment, the mobilEcho Administrator behaves differently than it does in a non-clustered environment. You should always execute administration tasks on the node currently running the mobilEcho Virtual Server you want to administer. Starting the service from the mobilEcho Administrator or the Services control panel is disabled for clustered configurations.

Clustered services should be started ONLY from the Microsoft Cluster Administrator. If the service is started by some other means (an application or the Services control panel) the Cluster Administrator will not know the service is running and, if required, cannot manage a failover.

Administer services only from the node they are running on. Then, you can create volumes that point to a specific folder. On a cluster, a node can only access the disks in its cluster group. In order to select a folder with the Browse for folder dialog you must run the mobilEcho Administrator on the node where the Physical Disks are located. Using the mobilEcho Administrator, you can create a volume on another node; however, you will need to enter the path manually.



When the mobilEcho Administrator is started, you will be prompted to select the mobilEcho service that you want to administer. Select a mobilEcho Service and click **OK**.

Once you have chosen a service, the Administrator launches and connects to that service. The Administrator title bar tells you which server it is connected to in the format “(Network Name – Service Name)”.

If the connection to the server is broken (that Cluster Group is failed over) the Administrator cannot reconnect to that service since it is on another node. However, you can now administer it on the node to which it has been moved. If it fails back to the original node, you can reconnect to it.

Setting up mobilEcho Client Management on a Cluster

If you choose to enable the mobilEcho Client Management Server on a cluster, you will need to manually create the **mobilEcho Management** service on each node. Before you do this, you will need to prepare the cluster by moving the mobilEcho Client Management servers configuration and data files to shared storage that is accessible to all nodes of the cluster.

Configuration and data file requirements

The mobilEcho Client Management Server uses a set of configuration files, policy files, and a database to store its configuration and details about the client devices that are enrolled in the mobilEcho management server. On a cluster, these data files must be relocated from their default location, within the mobilEcho Program Files directory, to a shared storage location on the cluster. This allows the unique set of data files to remain available when the mobilEcho Client Management service is moved between different cluster nodes.

Copying the configuration and data files to shared storage

When you initially installed mobilEcho on your cluster, a default set of configuration and data files was created in the mobilEcho "Program Files" directory, typically each cluster node's Windows OS drive. This set files needs to be moved to a shared storage drive on your cluster that is accessible by all of the individual cluster nodes. This is required so that the mobilEcho Client Management Server service can be failed over between nodes and retain the same configuration and database. If this is not done, the mobilEcho Client Management server will revert to it's default, unconfigured state when it fails over to a new node.

To copy your configuration and data files to shared storage:

1. Pick a cluster node to copy the files from. If you just installed mobilEcho on all cluster nodes for the first time, you can pick any node you like. If you've already started configuring the mobilEcho Client Management service on a particular node, you'll want to copy the files from that specific node.
2. Pick a shared storage location that all cluster nodes have access to.
3. In this location, create a folder to place the configuration and data files in. In this example, I'm going to use a shared storage "S: drive" and create a folder in the root of that drive called "**mobilEcho_Config**".
4. Open the "**mobilEcho_Config**" folder and create a new folder inside of it called "**ManagementUI**".
5. From the chosen cluster node, copy the **mobilEcho_manager.cfg** file from its original location (C:\Program Files (x86)\Group Logic\mobilEcho Server\ManagementUI\mobilEcho_manager.cfg) to the new "**ManagementUI**" folder on shared storage. When you've completed this step, you'll have an **S:\mobilEcho_Config\ManagementUI** directory with a **mobilEcho_manager.cfg** file in it.
6. From the chosen cluster node, copy the entire "**db**" folder into the "**ManagementUI**" folder on shared storage. The original location of this file on the cluster node is: C:\Program Files (x86)\Group Logic\mobilEcho Server\ManagementUI\db\. When you've completed this step, you'll have an **S:\mobilEcho_Config\ManagementUI\db** directory with several database files in it.
7. From the chosen cluser node, copy the entire "**Management**" directory into the "**mobilEcho_Config**" folder. The original location of this file on the cluster node is: C:\Program Files (x86)\Group Logic\mobilEcho Server\Management\. When you've completed this step, you'll have an **S:\mobilEcho_Config\Management** directory with several database files in it.

Configuring the mobilEcho Client Management service to use the new data file location

In order for each individual mobilEcho Client Management Service on each cluster node to know to use the new shared configuration and data file location, a config file will need to be edited on each node of the cluster.

On each individual cluster node:

1. Navigate to the **C:\Program Files (x86)\Group Logic\mobilEcho Server** folder.
2. Open the **config.yml** file in a text editor.
3. There are 4 settings in this file that will need to be updated:
    a. **config_path** - Enter the full path of the ManagementUI folder you created on shared storage. It is recommended you use forward slashes in all these paths.
    b. **database_path** - Enter the full path of the db folder on shared storage.
    c. **management_path** - Enter the full path of the Management folder on shared storage.
    d. **profiles_path** - Enter the fill path of the Profiles folder on shared storage.
4. Here's an example of how these settings look for the S: drive example locations above. Make sure to use a full path, starting with the drive letter of the shared storage location. Again, we recommend you use forward slashes in these paths in the **config.yml** file.

```
###
# Location of the folder containing the mobilEcho_management.cfg file.
# Default value: "."  (ManagementUI folder)
# Example full path value: "S:/mobilEcho_Config/ManagementUI/"

config_path: "S:/mobilEcho_Config/ManagementUI/"

###
# Location of the database file used by the Rails management app.
# Default value: "./db/"  (relative to ManagementUI folder)
# Example full path value: "S:/mobilEcho_Config/ManagementUI/db/"

database_path: "S:/mobilEcho_Config/ManagementUI/db/"

###
# Location of the management folder.  This folders includes the priority.txt file used to store group priority
order.
# Default value: "../Management/"  (relative to ManagementUI folder)
# Example full path value: "S:/mobilEcho_Config/Management/"

management_path: "S:/mobilEcho_Config/Management/"

###
# Location of the profiles folder.  This folder includes the individual group and user profile files.
# Default value: "../Management/Profiles/"  (relative to ManagementUI folder)
# Example full path value: "S:/mobilEcho_Config/Management/Profiles/"

profiles_path: "S:/mobilEcho_Config/Management/Profiles/"
```

5. Once your edits have been made, save the **config.yml** file.
6. If the **mobilEcho Management** service is currently running on this node, it will need to be restarted before these changes take effect.
7. You will need to edit this file on each node on the cluster. You can simply copy the edited file from this first node to each additional node and overwrite the existing file if you like. Make sure you restart the service on each node if it happens to be running.
8. The **mobilEcho Management** service can now be moved between cluster nodes and retain the same set of configuration and data files.

Configuring the inital mobilEcho Client Management Server settings

Before you create the **mobilEcho Management** service, you will need to update the mobilEcho Client Management configuration file that's now located on shared storage. See the Client Management Server section of this manual for further details.

Create the mobilEcho Management service on each node

To create the **mobilEcho Management** service:

1. Log into the relevant cluster node

2. Open the Windows command prompt

3. On 32-bit versions of Windows, enter:

- sc create “mobilEcho Management” binpath= “C:\Program Files\Group Logic\mobilEcho Server\mobilEcho_management.exe”

4. On 64-bit versions of Windows, enter:

- sc create “mobilEcho Management” binpath= “C:\Program Files (x86)\Group Logic\mobilEcho Server\mobilEcho_management.exe”

mobilEcho File Server

Starting and Stopping the mobilEcho File Server

To start the mobilEcho File Server, log into Windows with administrator privileges and launch the mobilEcho Administrator. If the mobilEcho service has not already started, the mobilEcho Administrator asks if you want to start the service.

In addition, you can start and stop the service from the Windows Service Control Panel on a standalone server or the Cluster Administrator on a cluster server.

Configuring the mobilEcho Server

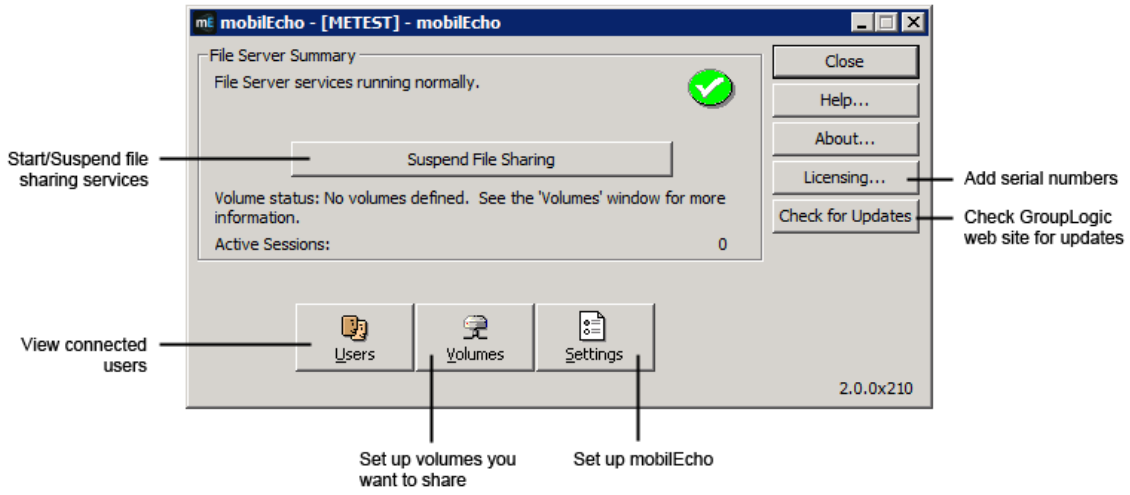
This section gives an overview of configuring the mobilEcho service. Use the mobilEcho Administrator to view connected users, create shared volumes, and adjust specific machine settings. You can configure the local computer or remote computers on which mobilEcho is installed as long as you have administrative privileges.

To configure mobilEcho on the computer you are using, from the Windows **Start** menu, go to **Programs/ mobilEcho Server** and **select mobilEcho Administrator**.

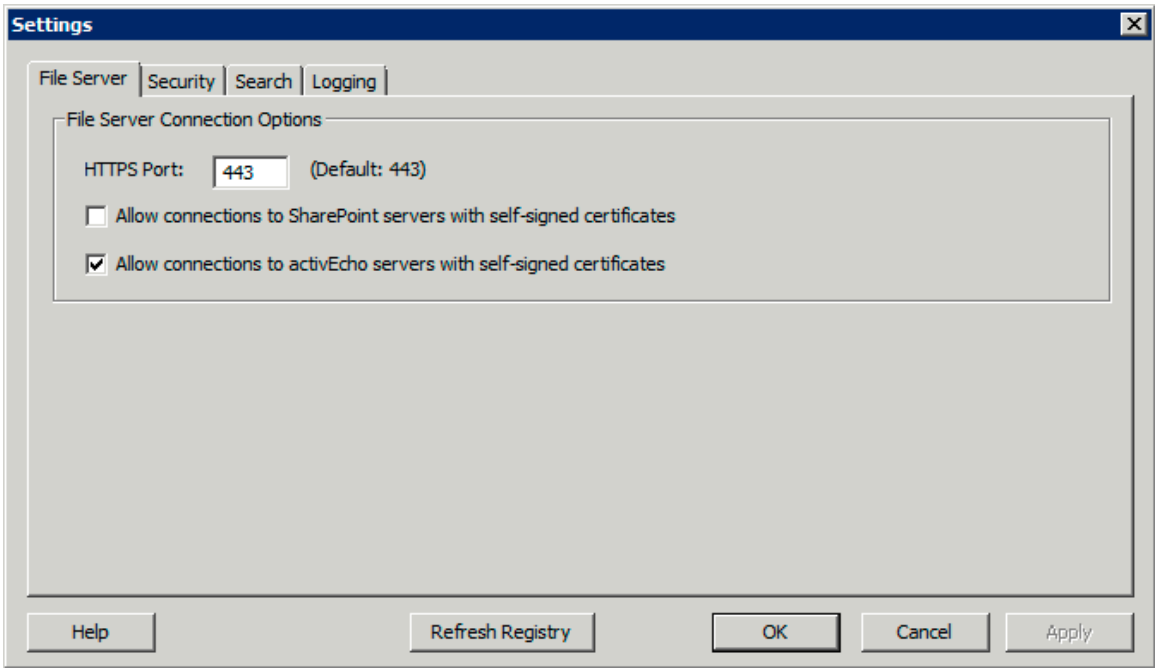
Setting up mobilEcho

Before using mobilEcho, review the default settings; you can make changes at this time or later. The **Setti ngs** dialog box has the following tabs: **File Server**, **Security**, **Search**, and **Logging**. To change settings, do the following:

1. Access the **mobilEcho Administrator** window.
2. Click **Settings**.
3. Choose the settings appropriate for your use, then click **OK** to return to the mobilEcho Administrator window.



Setting File Server Options



HTTPS Port

If you require mobilEcho to operate on a port different from the default HTTPS port, 443, it can be configured here. mobilEcho clients connecting to a server with a non-default port will need to specify the port in the server name or IP address when they are configured. For example, if port 444 is used, ":444" would need to be appended to the server name. In this example, the server name entered would be: server.domain.com:444

Allow connections to SharePoint servers with self-signed certificates

mobilEcho can be configured to provide access to files located on SharePoint servers. If any SharePoint servers your users will access are using self-signed certificates, the mobilEcho server needs permission to connect to these SharePoint servers, despite the lack of a trusted 3rd party issued certificate. Enable this setting to allow access to SharePoint servers using self-signed certificates.

Allow connections to activEcho servers with self-signed certificates

mobilEcho can be configured to provide access to users' files located activEcho servers. If your activEcho server is using a self-signed certificate, the mobilEcho server needs permission to connect to this activEcho server, despite the lack of a trusted 3rd party issued certificate. Enable this setting to allow access to activEcho servers using self-signed certificates.

Using mobilEcho to provide mobile access to activEcho servers

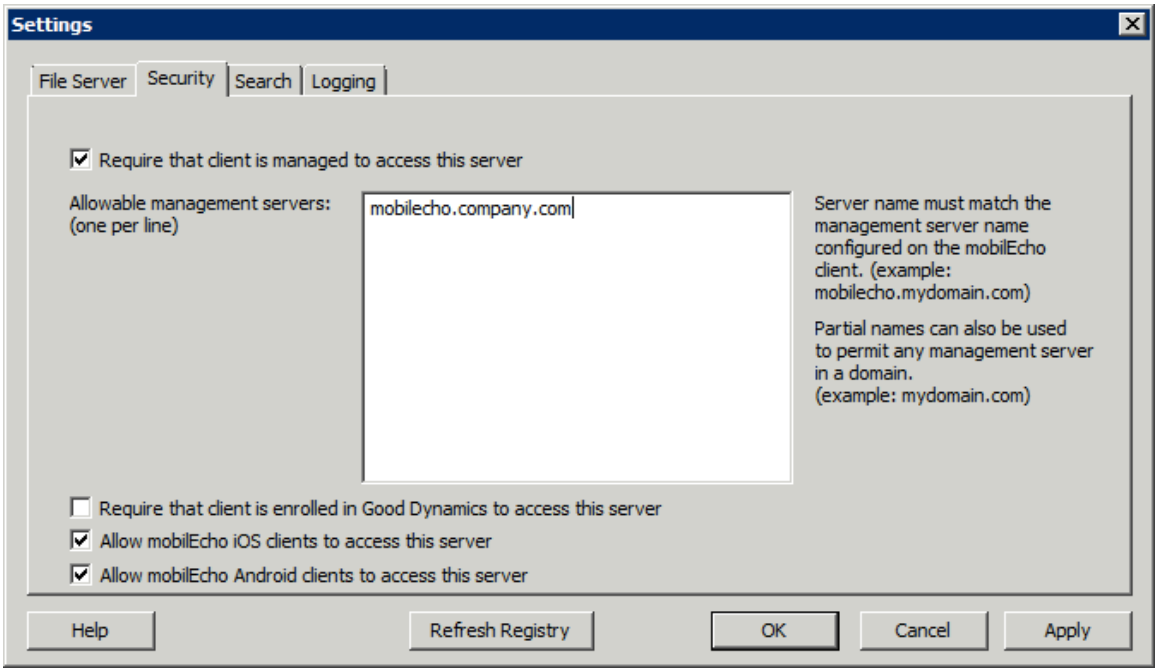
A mobilEcho server is capable of giving access to activEcho files to mobile devices running the mobilEcho client app. This capability is configured by creating an activEcho volume in the mobilEcho Administrator **Volumes** window. In the mobilEcho client app, the activEcho volume is presented just like a standard mobilEcho volume, but is distinguished with a special activEcho icon. When the user connects to this activEcho volume, they will see only the activEcho folders that their account has access to.

The mobilEcho server does not require a mobilEcho serial number to allow activEcho volumes to be created. This **activEcho volumes** feature is included in the activEcho retail license. If a mobilEcho server trial expires and that server is configured to share activEcho volumes, those activEcho volumes will continue to allow users to connect indefinitely.

Refresh Registry button

The **Refresh Registry** button is used to apply changes that have been made directly to mobilEcho's registry key settings. Changes made to registry key settings typically do not take effect until after the mobilEcho File Server service is restarted. You can avoid a service restart and apply these changes immediately by clicking **Refresh Registry**. This is only necessary if you change mobilEcho settings directly in the registry.

Setting Security Options



Require that client is managed to access this server

If you select this option, all mobilEcho clients connecting to this server are required to be managed by a mobilEcho Client Management Server that is listed under **Allowable management servers**. This option ensures that all clients accessing the server have the settings and security options you require.

The server name entered here must match the management server name configured in the mobilEcho client app. Partial names may also be used to allow multiple client management servers in a domain, for instance. Partial names do not need wildcard symbols.

Require that client is enrolled in Good Dynamics to access this server

If you select this option, only mobilEcho clients that are enabled for and enrolled in Good Dynamics will be allowed to connect to this mobilEcho server. This setting can be used to ensure that all clients accessing your mobilEcho server are members of your Good Dynamics system. If you enable this option, any existing users who are not enrolled in Good Dynamics will immediately be denied access to log into this server. Please note that the current mobilEcho for Android app does not support Good Dynamics. If you require Good Dynamics to access your server, Android clients will automatically be denied access.

Allow mobilEcho iOS clients to access this server

If you select this option, this mobilEcho server will allow users running the iOS mobilEcho client app to connect. If you do not want to allow iOS users to access this mobilEcho server, you can uncheck this setting.

Allow mobilEcho Android clients to access this server

If you select this option, this mobilEcho server will allow users running the Android mobilEcho client app to connect. If you do not want to allow Android users to access this mobilEcho server, you can uncheck this setting.

Searching with mobilEcho

mobilEcho performs three types of file searches – local searches, filename index searches, and content searches.

Local Search

If a mobilEcho server does not support filename index or content search, the mobilEcho client defaults to searching its local list of files, in current folder being browsed, by filename.

Filename Index Search

An index search issues a single search request that is processed on the server side.

By default, mobilEcho maintains a search index to accelerate these searches. This index contains the name of every file on your mobilEcho volumes. With indexed searching enabled on the server, a mobilEcho client can search both the currently browsed folder and the entire current shared volume. These results are delivered very quickly because they are processed on the server side.

Content Search

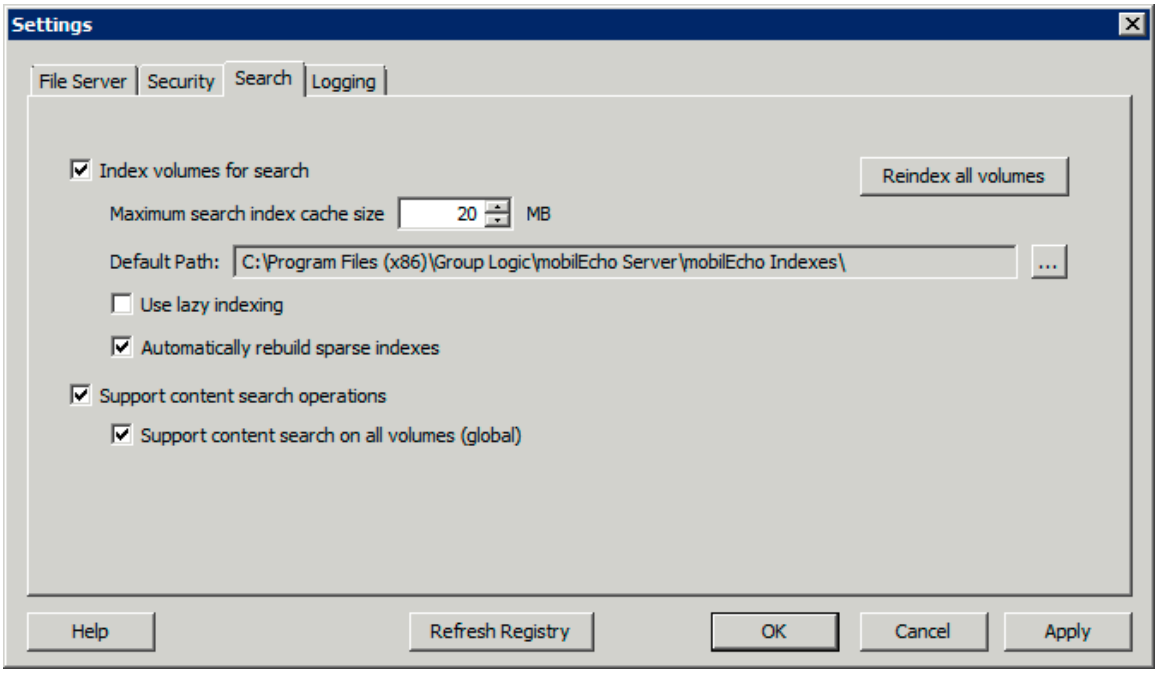
A content search issues a single search request that mobilEcho processes on the server side. A content search returns files that contain the requested search term, in either the filename or the actual contents of

the file.

Content search is enabled by default, but requires that the Windows Search service is enabled on the server and is configured to index the storage areas that are being shared as volumes by mobilEcho.

For instructions on installing and configuring Windows Search, please see GroupLogic's Network Spotlight Best Practices white paper. This document was authored for GroupLogic's ExtremeZ-IP File Server, which also uses Windows Search in much the same way. The section on enabling Spotlight search in ExtremeZ-IP can be skipped.

Setting Search Options



Index volumes for search

By default, indexed searching is enabled on all existing and newly created volumes. You can disable or enable indexed searching on a per volume basis in the individual volume's **Volume Properties** dialog in mobilEcho Administrator. You can set this property at initial volume creation time or after the volume has been created. In order for changes to this setting to take effect, you must **Restart** the volume.

Maximum search index cache size

This cache is set to a maximum size of 20 MB by default. GroupLogic does not recommend changing this cache size. An index file containing 250,000 files is only about 8 MB in size. Leaving the cache limit at the default setting gives sufficient performance in almost all cases. If the index files on disk are larger than search index cache size, the file will be read from disk when the client does a search; however in many cases the file will be in the Windows file system cache so performance impact is minimal. When the server is running with limited physical memory, the cache size can be reduced to as little as 8 MB.

Default Path

By default on a standalone server, mobilEcho stores index files in the mobilEcho Indexes directory in the mobilEcho Server application folder. If you would like to locate the index files in a different location, click **Browse** to select a new folder.

Administrators can also specify custom index file paths for individual volumes; this setting overrides the global default path setting.

Use lazy indexing

By default, indexed searching uses any available system resource to keep its indexes current and cooperates with other system processes. It should not affect overall system performance adversely. However, when a server is under high load or is running many different services simultaneously, you can limit the system resources that search indexing consumes by enabling the **Use lazy indexing** checkbox. This setting takes effect immediately.

Automatically rebuild sparse index

In order to optimize runtime performance, the mobilEcho index file entries for files that have been deleted or moved from a volume are not physically removed from the index file at the time the actual file is deleted. The indexed search service ignores these deleted entries to keep search results accurate. However, the index file grows over time and, as the file gets larger, slows search performance to a small extent. The rate at which the index file grows is dependent on the number of files being added, moved, and deleted on the file server. In order to keep mobilEcho search performing at optimal levels, volumes' indexes are routinely re-indexed and compacted. The interval at which this occurs is determined by the ratio of deleted (stale) records to valid entries in the index. By default, the mobilEcho search service re-indexes an individual volume when approximately one-third of that volume's index file records are deleted, stale records.

Maintenance occurs on a per volume basis and only on volumes requiring re-indexing. While re-indexing, the volume's existing search index is kept up to date and used to provide one hundred percent accurate search results. Re-indexing should not have any detrimental effect on other server processes while it is running. While mobilEcho is re-indexing an individual volume, a status of "Reindexing" shows in the **Volumes** dialog of the mobilEcho Administrator.

Support content search operations

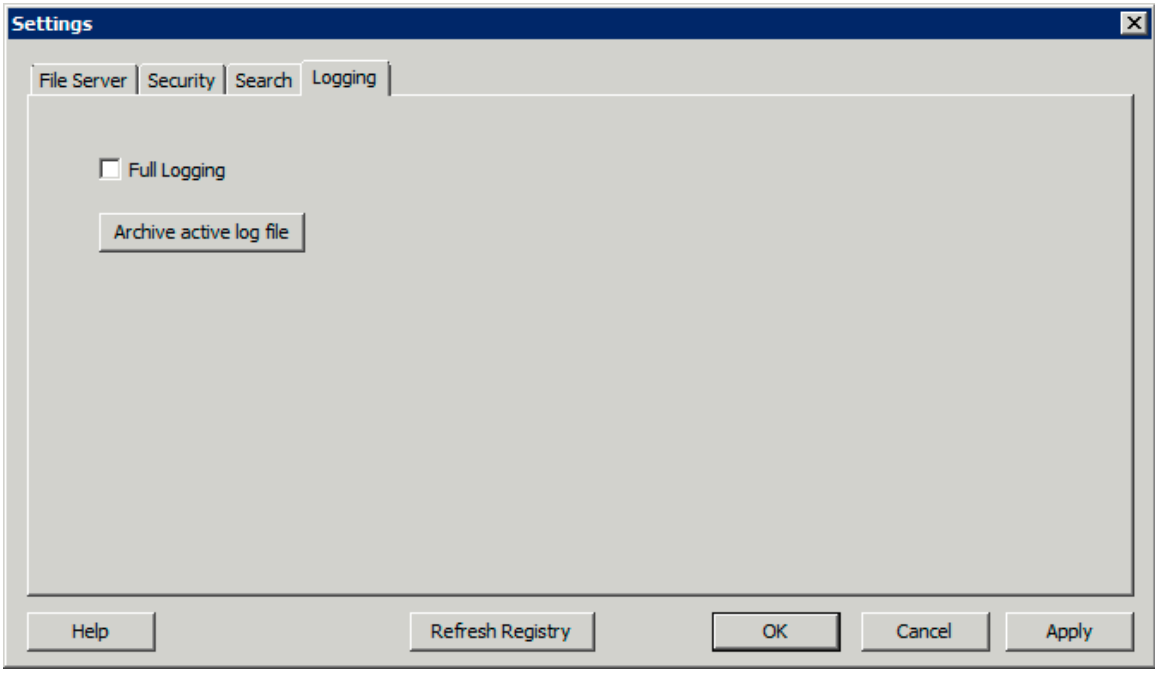
Support for content search of shared volumes is enabled by default, and can be enabled or disabled by checking this option. You can enable or disable content searching on a per volume basis in the individual volume's **Volume Properties** dialog. You can set this property at the time of initial volume creation or after the volume has been created. Enabling this setting takes effect for all new sessions using the volume.

In addition to enabling this setting, content search requires that the Microsoft Windows Search application be installed on the mobilEcho server and be configured to index any volume where content search is enabled. Windows Search is built into Windows Vista and no additional installation is required. It is also built into Windows Server 2008, but it is not enabled by default. To enable it add the Role called File Services in the Server Manager, and have the Windows Search Service enabled. Windows Search can be installed on Windows 2003 Server and Windows XP by running Windows Update. It is listed as an optional install. Once installed, Windows Search can be configured to index the necessary volumes by right clicking the Windows Search icon in the Start bar and selecting **Windows Search Options**.

Support content search on all volumes

To support content search on all volumes, check this box.

Setting Logging Options



Full Logging

When enabled, **Full Logging** increases the level of detail recorded in the mobilEcho log file. This is typically only needed when working with GroupLogic technical support. Enabling full logging could potentially have an impact on performance and should be used only for troubleshooting.

Archive Active Log File

Click this button to ZIP archive the current mobilEcho log file and start a new log file. This can be used to reduce the size of your existing log file for archiving or to package your log file for delivery to GroupLogic technical support. Log files are located in the \Program Files\Group Logic\mobilEcho Server\Logs\mobilEcho\ folder on your system drive by default.

Adding License Numbers

Using the **Licensing** button on the mobilEcho Administrator window, you can enter the serial number for any licenses without stopping the mobilEcho service. When you enter license numbers while the mobilEcho service is running, mobilEcho clients stay connected and continue to use mobilEcho volumes.

You need to enter license numbers when:

- you have a trial version of mobilEcho installed and you purchase a license for the product.
- you are upgrading your user count.
- you are converting from standalone server licensing to perpetual or annual enterprise licensing.

To add a serial number, do the following:

1. Open the mobilEcho Administrator application.
2. Click **Licensing** on the main mobilEcho Administrator window.
3. Click **Add License**, enter the serial number, and click **OK**.
4. The serial number will be displayed in the **Active Licenses** list and will take effect immediately.
5. Click **Close** to return to the mobilEcho Administrator.

The Licensing window can also be used to replace serial numbers to upgrade user count.

Administering mobilEcho Remotely

You can configure mobilEcho on a remote computer if mobilEcho is already installed on that computer. You must have Windows administrative privileges on the remote computer. The experience of administering a remote server is very similar to that of the local server Administrator, except that the title of the Administrator dialog box shows the name or IP Address of the remote computer whose mobilEcho service you are configuring and you cannot browse for folders to share. Otherwise, you can configure the remote server just as you would a local server.

To administer a remote mobilEcho server, do the following:

1. Hold down the **Control** key while you launch the mobilEcho Administrator. Alternatively, if there is no local installation of mobilEcho, mobilEcho Administrator will start immediately in remote mode.
2. Type the name or IP Address of the remote computer and click **OK**.
3. The mobilEcho Administrator will attempt to use your Windows credentials to log onto the server. If necessary, you will be prompted for an alternate username and password.

Using the mobilEcho File Server

After using the mobilEcho **Settings** dialog box to set up your server, security and search settings, you can create the volumes you want to share to you mobilEcho clients. You can also use the **Users** dialog box to see who is connected to the server.

Creating Volumes in mobilEcho

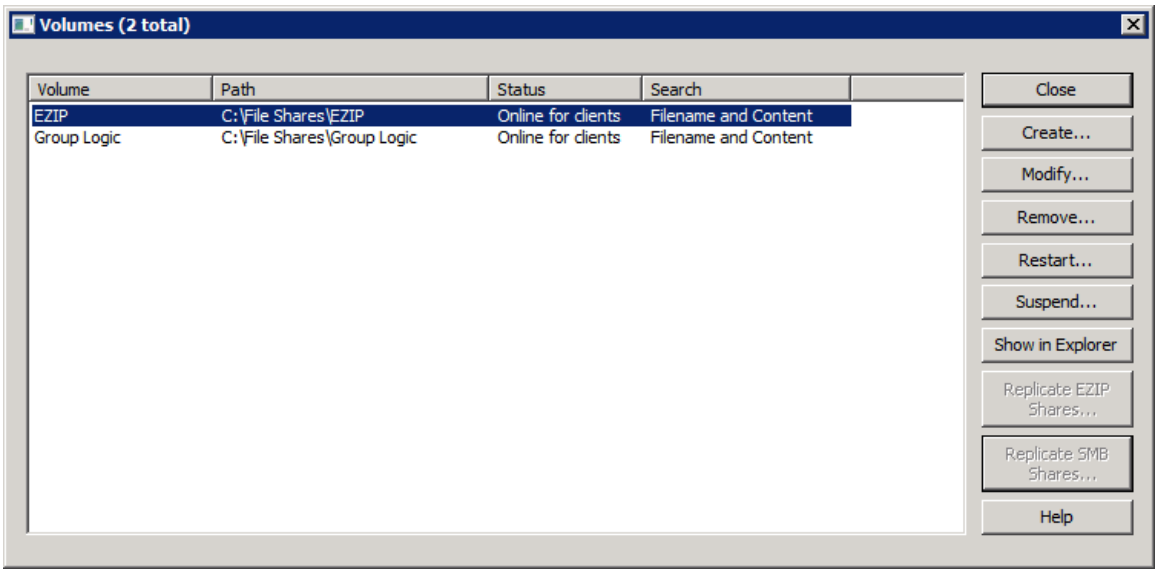
You can share NTFS directories located on your Windows server, or on a remote SMB/CIFS file share, for access by mobilEcho users. When mobilEcho users connect, they see these directories as file share volumes.

You can create volumes that provide access to an **activEcho** server.

You can also create volumes that provide access to a **SharePoint 2007 or 2010** server, site, subsite, or document library. Volumes that point to an entire SharePoint server, or an individual site or subsite, allow the user to browse and navigate through sites, subsites, and document libraries they have access to.

Use the **Volumes** dialog box to create, modify, or delete individual volumes to share with mobilEcho users.

Click **Volumes** on the mobilEcho Administrator main window to display the **Volumes** dialog.



Note:

You cannot create a volume with the name ***enroll***. This name is reserved for internal use.

Creating a Volume for a local folder or to re-share a location on another SMB/CIFS server

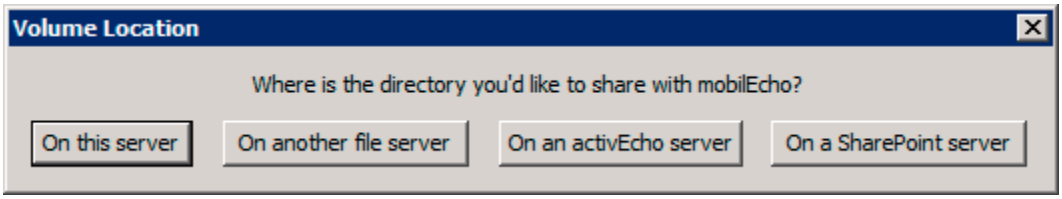
Folders residing directly on the Windows server running the mobilEcho server software can only be shared as mobilEcho volumes if they reside on an NTFS formatted disk. If you try to create a volume that is not on an NTFS formatted disk, mobilEcho will display an error message.

1. Create a new directory on an NTFS formatted volume on the server machine or find an existing directory that you want to use.

2. From the mobilEcho Administrator window, click **Volumes**.

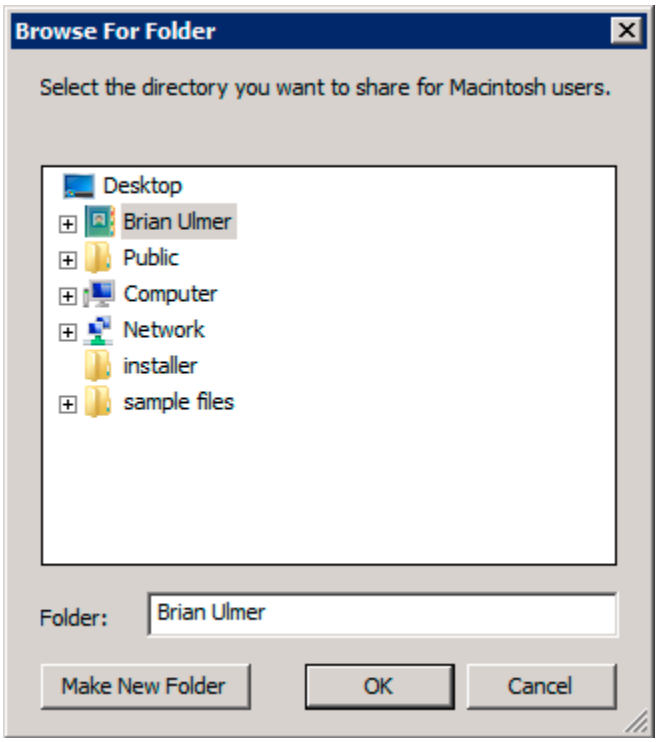
3. On the **Volumes** dialog, click **Create**.

4. If you are running a Trial or Enterprise License version of mobilEcho Server, you will be asked to choose a volume location. If you want to share files on this server's physical storage, choose **On this server**. If you want to share an SMB/CIFS volume located on another server or NAS device, choose **On another server**.



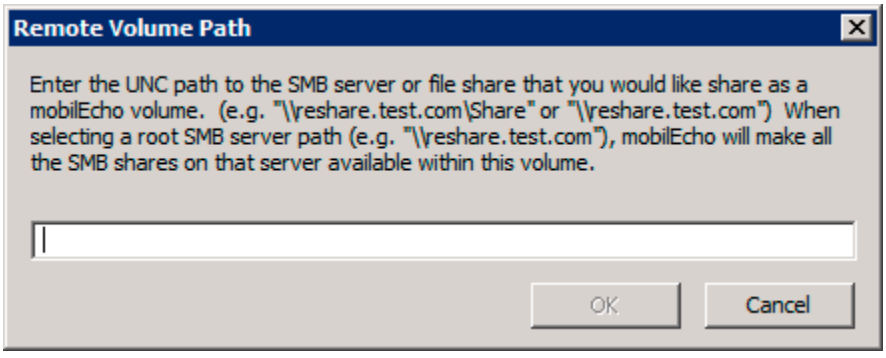
If you choose **On this server**, you will be prompted to select a directory location on this server. Browse to the path of the folder you want to share and click **OK**.

If you are running a mobilEcho Server with a non-enterprise perpetual license that does not support resharing volumes on other servers, you will not see options for creating a volume that resides on another file server or on a SharePoint server.

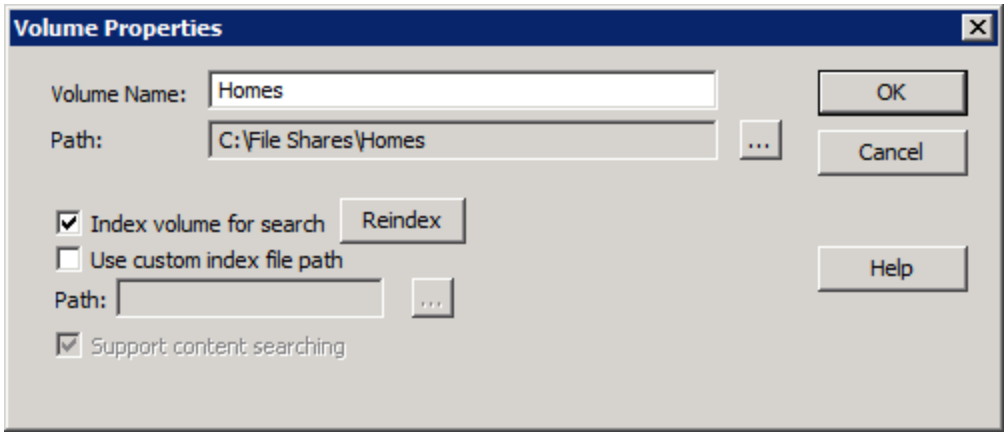


If you choose **On another server**, you will be prompted to enter the path to the server or SMB share you'd like to make available with this mobilEcho volume. Enter the desired path and click **OK**.

> **Microsoft Distributed File System (DFS) namespaces**
>
> mobilEcho's network reshare feature can be used to make DFS namespaces available to mobilEcho users. Simply specify the DFS namespace's path when creating an **On another server** volume.



5. The Volume Properties window will appear.



6. Edit the **Volume Name** if you want to change the name.

7. Choose any additional settings required. Search index settings only apply to volumes pointing to folders on the local Windows server.

8. Click **OK** to create the volume.

As soon as a volume's status becomes **Online for clients**, mobilEcho clients can see and connect to it.

> **File search on volumes with remote paths**
>
> The mobilEcho search indexing service and Windows Search integration runs on each of your servers where mobilEcho is installed. When a mobilEcho volume is configured for a path **On another server**, these local services are not able to index the remote server. For this reason, indexed filename and content search will be disabled for all volumes with remote network paths. Users will continue to be able to search the folder they are browsing by filename from within the mobilEcho client application.

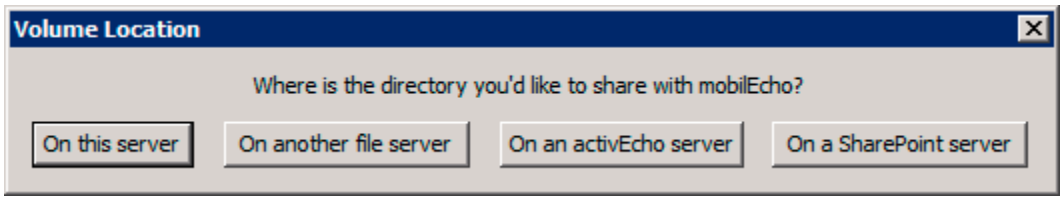
Creating a Volume that provides access to an activEcho server

The mobilEcho client app can be used to access and work with files on an activEcho server. When a mobilEcho user connects to an activEcho volume, they see the same set of files and folders that they have access to using the activEcho web interface. activEcho volumes simply need to point to the root HTTPS URL of an activEcho server.

1. From the mobilEcho Administrator window, click **Volumes**.

2. On the **Volumes** dialog, click **Create**.

3. To share an activEcho server, choose On an activEcho server.

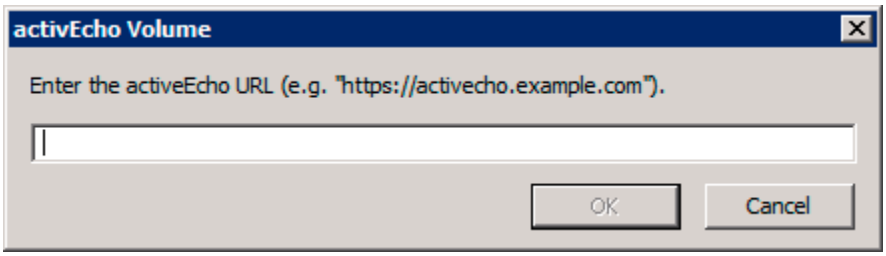


If you are running a mobilEcho Server with a non-enterprise perpetual license that does not support resharing volumes on other servers, you will not see options for creating a volume that resides on another

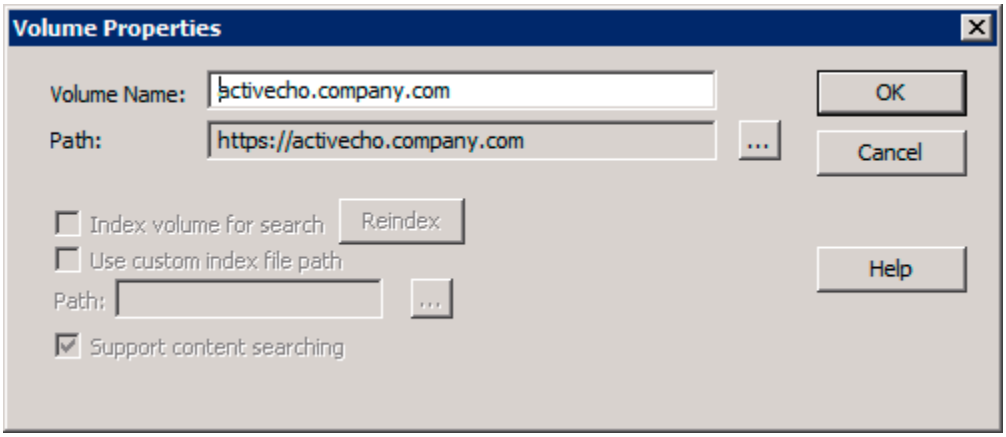
file server or on a SharePoint server.

4. Enter the HTTPS URL to the root of the activEcho server you would like this volume to provide access to.

> **Important Note: Requirement for SSL certificate may need to be modified**
>
> mobilEcho accesses activEcho servers using a standard HTTPS connection, just like a user does from a web browser. If your activEcho server is not configured with a valid 3rd party SSL certificate, mobilEcho needs permission to allow this connection.
>
> If your activEcho server uses a self-signed certificate, you will need to enable **Allow connections to activEcho servers with self-signed certificates** on the **File Server** tab of the **Settings** window.



5. The **Volume Properties** window will appear.



6. Edit the Volume Name if you would like to change the name.

7. Click OK to create the volume.

Creating a Volume that provides access to SharePoint 2007 or 2010 content

mobilEcho can provide access to files residing in **document libraries** on SharePoint 2007 and 2010 servers. A mobilEcho SharePoint volume can point to an entire SharePoint server, a specific SharePoint **site** or **subsite**, or a specific **document library**. These files can be previewed, PDF annotated, edited, and synced, just like files that reside in traditional file server or NAS storage. mobilEcho also supports **Ch eck Out** and **Check In** of SharePoint files.

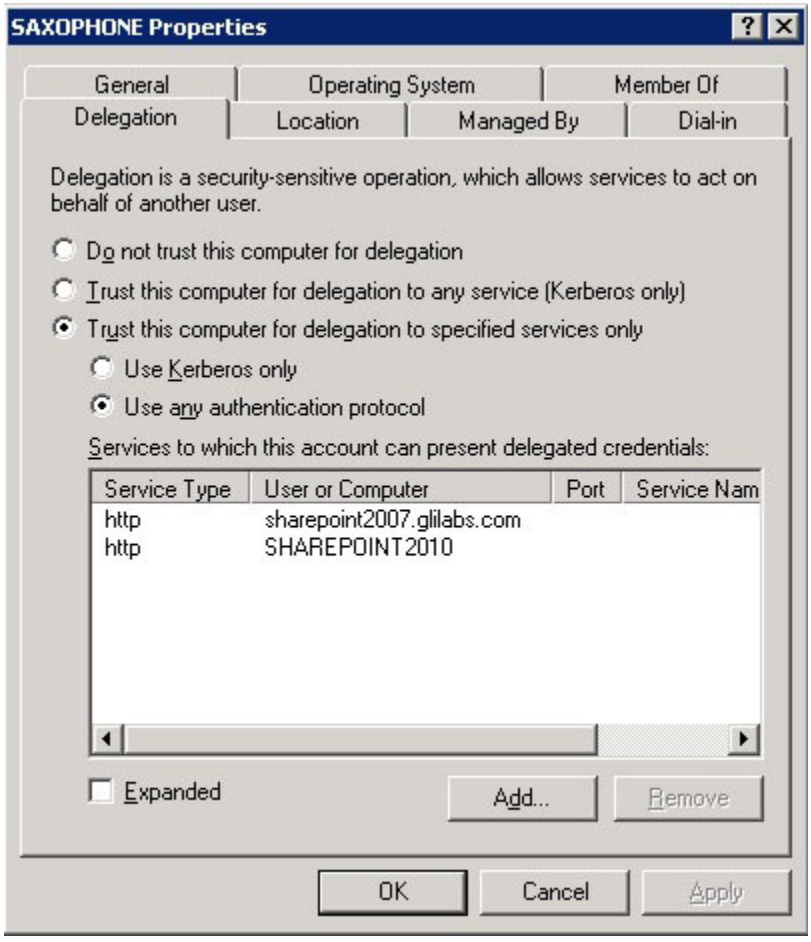
SharePoint authentication methods supported

mobilEcho supports SharePoint servers that allow client authentication using **NTLMv1**, **NTLMv2**, and **Ker**

beros. If your SharePoint server requires Kerberos authentication, you will need to make an update to the Active Directory computer object for the Windows server or servers that are running the mobilEcho server software. The mobilEcho Windows server needs to be given permission to present delegated credentials to your SharePoint server on behalf of you users.

Enabling the mobilEcho Windows server to perform Kerberos Delegation

1. In **Active Directory Users and Computers**, locate the Windows server or servers that you have mobilEcho installed on. They are commonly in the **Computers** folder.
2. Open the **Properties** window for the Windows server and select the **Delegation** tab.
3. Select "**Trust this computer for delegation to specified services only**"
4. Select "**Use any authentication protocol**", this is required for negotiation with the SharePoint server.
5. You must now add any SharePoint servers that you would like your users to be able to access using mobilEcho. If your SharePoint implementation consists of multiple load balanced nodes, you will need to add each SharePoint/Windows node to this list of permitted computers. Click **Add...** to search for these Windows computers in AD and add them. For each, you will need to select the "**http**" service type only.
6. Please allow 15 to 20 minutes for these change to propagate through AD and be applied before testing client connectivity. They will not take effect immediately.

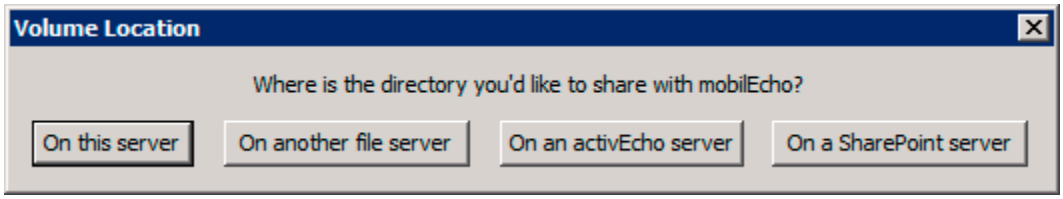


To configure a SharePoint volume on the mobilEcho server:

1. From the mobilEcho Administrator window, click **Volumes**.

2. On the Volumes dialog, click Create.

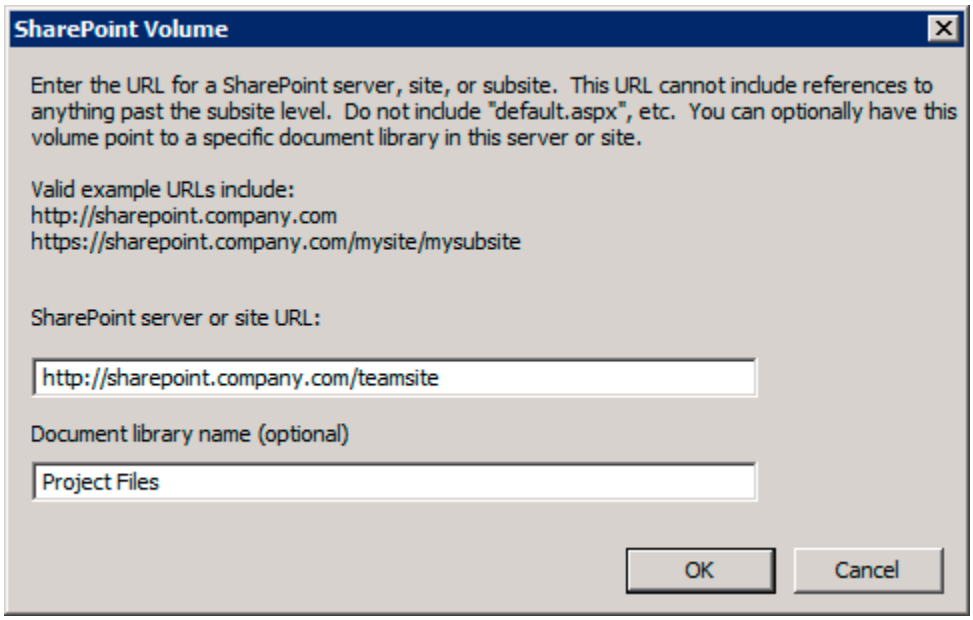
3. If you are running a Trial or Enterprise License version of mobilEcho Server, you will be asked to choose a volume location. To share a SharePoint server, site, or document library, choose On a SharePoint server.



If you are running a mobilEcho Server with a non-enterprise perpetual license that does not support resharing volumes on other servers, you will not see options for creating a volume that resides on another file server or on a SharePoint server.

4. You are prompted to enter the URL of the SharePoint server, site, or subsite you would like this volume to point to. This is the same URL you would use in a web browser to access that server, site, or subsite. The URL can only include a SharePoint HTTP or HTTPS URL to the root location of the server or to the root location of a site or subsite. Do not use a URL path that includes a document library or other non-site folder name, or a file name like "default.aspx".

For volumes that point to a specific document library, after entering the URL to the site or subsite where the document library resides, enter the name of the document library in the Document library name field.



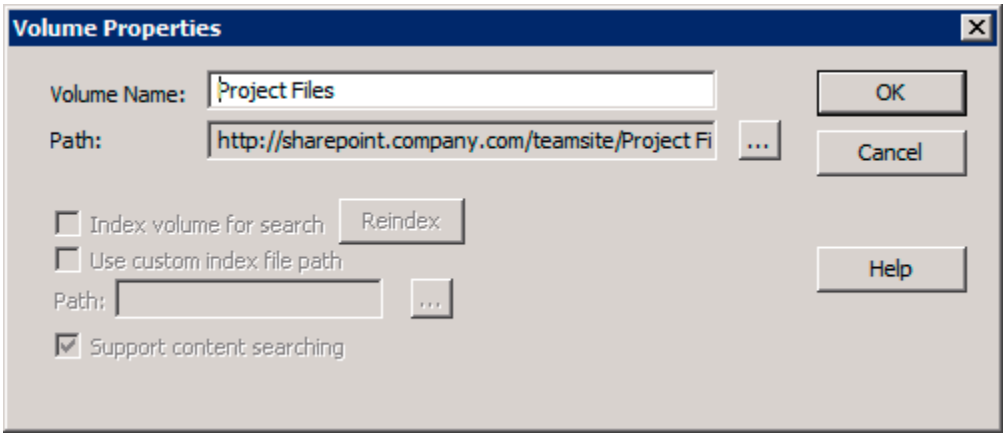
Required setting for HTTPS SharePoint servers with self-signed certificates

mobilEcho accesses SharePoint servers using SharePoint web services over a standard HTTP HTTPS connection, similar to how a user does from a web browser. If your SharePoint server is not configured with a valid 3rd party SSL certificate, and you've configured mobilEcho share an https:// SharePoint URL, mobilEcho needs permission to allow this connection.

Some SharePoint servers are configured to only allow HTTPS connections and will redirect any HTTP connections to HTTPS. In this scenario, if your SharePoint server is using a self-signed certificate, you will also need to give mobilEcho permission to allow this connection.

If your SharePoint server uses a self-signed certificate, you will need to enable **Allow connections to SharePoint servers with self-signed certificates** on the **File Server** tab of the **Settings** window.

5. The Volume Properties window will appear.



6. Edit the Volume Name if you would like to change the name.

7. Click OK to create the volume.

If you are using **Personal Sites** in your SharePoint configuration, you will not be able to browse them directly. If you add as a volume a specific SharePoint site, e.g. **http://sharepoint2010.glilabs.com:2229/my/personal/user**, it will just work. If the volume path leads to the folder above, e.g. **http://sharepoint2010.glilabs.com:2229/my/personal/** or **http://sharepoint2010.glilabs.com:2229/my/**, you will receive an error when trying to open that volume, but you'll be able to provision folders within that volume, either by path ("user") or by using the **%USERNAME%** wildcard.

Volume Properties

Index volume for search

Filename indexed searching is enabled on newly created volumes. To disable this feature, remove the check from this checkbox; in addition, you must **Restart** the volume in the **Volumes** dialog for this change to take effect.

Use custom index file path

To specify an alternate index file location for a volume, place a check in this checkbox and select a path for the new index file location.

Support content searching

Enables content searching on the volume by mobilEcho clients. This feature requires that Microsoft Windows Search is installed on the server. mobilEcho defaults to having content search enabled on all volumes. To disable it on an individual volume, you must first uncheck **Support content search on all volumes** on the **Search** tab of the **Settings** dialog.

> **Search Index and Content Search settings apply only to "On this Server" volumes**
>
> mobilEcho is only capable of tracking live changes to files that exist in the storage on the Windows server where mobilEcho is installed. For this reason, only volumes located on directly on the mobilEcho server support fast indexed filename search and Windows Search integrated full content search.

Changing Permissions for Shared Files and Folders

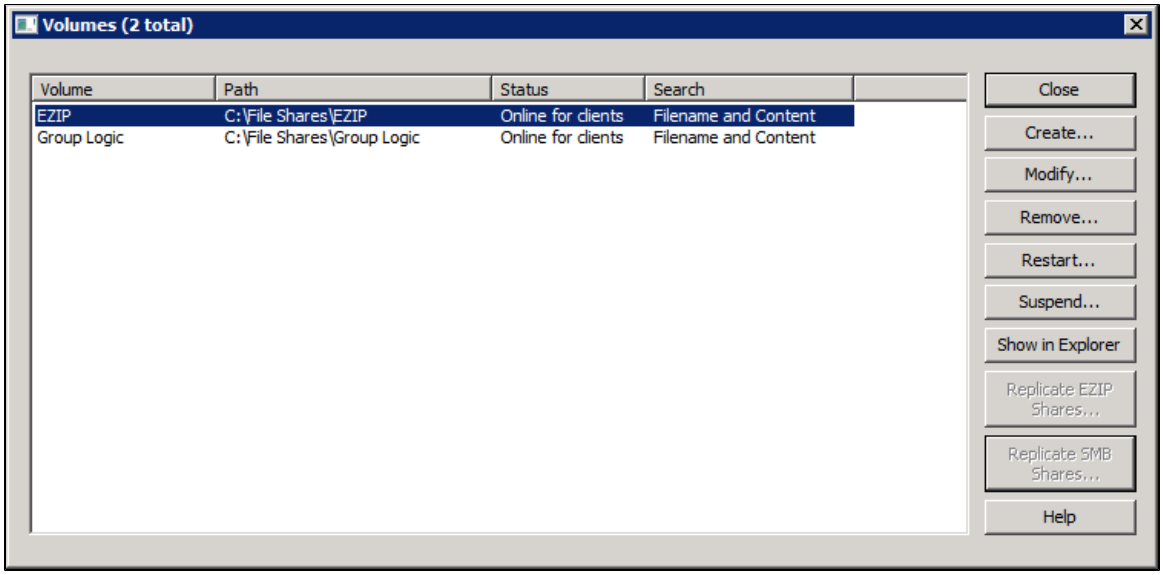
mobilEcho uses the existing Windows user accounts and passwords. Because mobilEcho enforces Windows NTFS permissions, you should normally use Windows' built-in tools for adjusting directory and file permissions. The standard Windows tools provide the most flexibility for setting up your security policy.

mobilEcho volumes that reside on another SMB/CIFS file server are accessed using an SMB/CIFS connection from the mobilEcho server to the secondary server or NAS. In this case, access to the secondary server is performed in the context of the user logged into the mobilEcho client app. In order for that user to have access to files on the secondary server, their account will need both "Windows Share Permissions" and NTFS security permissions to access those files.

Permissions to files residing on SharePoint servers are regulated in accordance to the SharePoint permissions configured on the SharePoint server. Users receive the same permissions through mobilEcho as they receive when they access SharePoint document libraries using a web browser.

Replicating Volumes

You may desire to make all your existing Windows File Shares or ExtremeZ-IP File Shares available to mobilEcho users. Each time you reopen the **Volumes** window, mobilEcho checks for any Windows SMB or ExtremeZ-IP AFP volumes that are not currently shared as mobilEcho volumes. If such volumes are found, the appropriate **Replicate** button is enabled.



When you click a **Replicate** button, the number of shares to be replicated is displayed and you are asked to verify that you want to replicate them.

Because someone could add or remove volumes to either the SMB or EZIP service at any time, when you reopen the **Volumes** window, note the state of the **Replicate** buttons. If they are dimmed (disabled), no new SMB or EZIP volumes have been added. If one of the corresponding mobilEcho volumes is removed, the button is enabled.

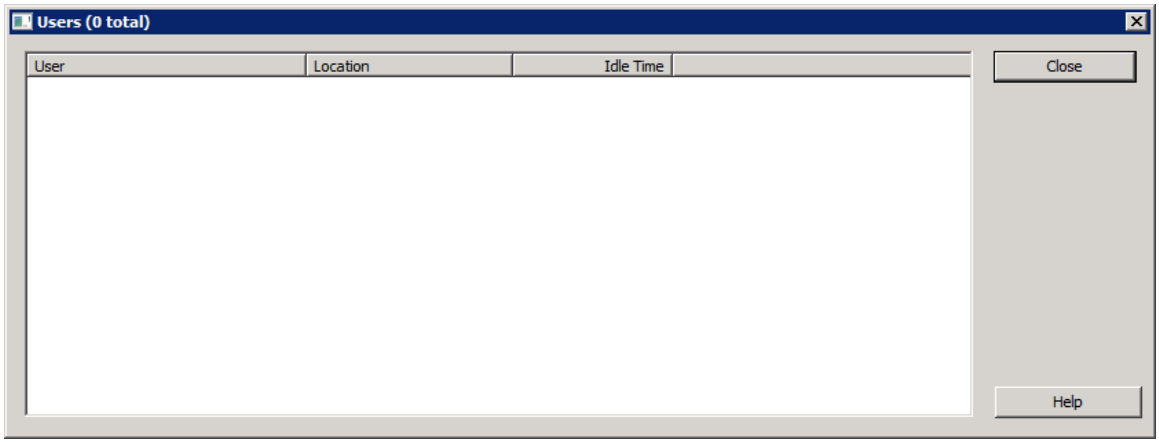
mobilEcho Users

The **Users** dialog box lets you view the users connected to the server.

To view the **Users** dialog box, click **Users** on the mobilEcho Administrator window.

User names and Location IP addresses identify users who are currently connected. Their idle times are also given. The dialog refreshes automatically.

Click on a column title to sort the list by a column.



Setting a minimum client version

Each mobilEcho file server contains a minimum client version setting. If a client of a version preceding the one set in that key attempts to connect to the mobilEcho server, it will receive a notice that it doesn't meet

the minimum version requirement and will be refused connection.

When mobilEcho is first installed, this minimum client version is set to the earliest version that is compatible with the mobilEcho server. If the server is later upgraded to a new version of the mobilEcho file server software, this minimum client version setting will be modified only if necessary for compatibility, which usually won't be the case.

If you would like to set the minimum client version that you allow to connect to you mobilEcho server, you can do so by editing this registry key:

\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\mobilEcho\Parameters4\Refreshable\Pez\MinimumClientVersion

The version number entered in this registry key needs to match the version number as it appears in the mobilEcho client app's settings menu. For example, the minimum client version number for mobilEcho 2.X and 3.X servers to date is: 2.0.0.282

If you have multiple mobilEcho servers, you will need to set this registry key on each server if you would like the minimum client version requirement enforced by each server. Alternatively, if you're using the mobilEcho Client Management system to centrally manage your clients, you can set this setting on just the server that is acting as the client management server. Since all your clients call home to this server, they will be denied access the next time they do and will be prompted that they need to upgrade their client app.

Clients not meeting the minimum version requirement will not receive updated profiles or remote wipe commands

If you set the minimum client version setting on your mobilEcho Client Management server, any existing managed clients that are running an earlier version of the mobilEcho app will no longer be able to communicate with the server to receive updated management profiles or remote wipe commands. If you need to remote wipe a client running an older version of the mobilEcho app, you will need to modify this setting so that it's allowed to communicate with the server.

mobilEcho Client Management Server

Introduction

mobilEcho Client Management Server provides comprehensive tools that allow you control and track the devices that access your mobilEcho servers. This includes the ability to create mobilEcho client policies that regulate the settings and capabilities of your mobilEcho clients. These tools ensure IT has full control over secure mobile device access to corporate files.

Client Management options include:

- Device level tracking and status
- PIN-based mobilEcho client enrollment can be required for client access
- User profiles
- Group profiles
- Client app password lock policies
- Application-level file permission policies (view, edit, create, delete, rename)
- Application-level file distribution policies (allow emailing, printing, editing in other applications, annotation, etc.)
- Caching policy
- Assignment of servers, folders, and home directories displayed in the client application
- Whitelisting and blacklisting of third party apps allowed to open mobilEcho files
- Remote application lock password reset

- mobilEcho app-specific remote wipe capability

mobilEcho Client Management allows profiles to be assigned to Active Directory users or groups. Group profiles are assigned an order of precedence and a user is governed by the highest priority group profile they are a member of. In the case that a specific user needs a special set of capabilities, user profiles can be created and take precedence over group profiles, ensuring that the user gets the profile settings required.

Once mobilEcho Client Management profiles have been established, the IT administrator invites users to activate their mobilEcho client app by using the mobilEcho Client Management Administrator to email them a mobilEcho Enrollment Invitation. If two-factor client enrollment is desired, this invitation email can optionally contain a one-time use PIN number, required to enroll the device in your mobilEcho management system. From their device, the user simply taps a link in the enrollment email which launches the mobilEcho app and automatically starts the enrollment process. The user is then asked to enter their Active Directory account password. If PIN number and account credentials are valid, the user is asked to set an application lock password if required, warned of any restrictions that will remove existing files from the device, and from that point on, the mobilEcho client application is managed by established management profile settings. Each time the mobilEcho client is started, it calls home to the Client Management Server and is updated with any settings changes or assigned servers that have been added or removed from the profile.

As a complement to mobilEcho Client Management, administrators can also use a Mobile Device Management (MDM) system to enforce iOS level policies for corporate devices. For example, you can require the use of an iOS Passcode Lock through an iOS Configuration Profile set up through an MDM server. The profile can also be configured to require that any device data backed up through iTunes will be encrypted on the computer. For more information about Mobile Device Management, see http://www.apple.com/ipad/business/integration/mdm.

Enabling the mobilEcho Client Management Server

If you wish to remotely manage your mobilEcho clients, at least one mobilEcho Server must have its **mobilEcho Client Management Server** component enabled. The mobilEcho Client Management Server is installed when you install mobilEcho Server, but is disabled by default. Even if you have many mobilEcho file servers, it is typical to maintain only one mobilEcho Client Management Server that manages all your mobilEcho clients. The selected server can act as a file server and management server simultaneously and can handle thousands of clients.

If you are deploying mobilEcho across widely separated geographical locations or in multiple departments with unique IT policies or Active Directory structure, multiple mobilEcho Client Management Servers can be configured as needed.

> **Domain Membership**
>
> Your client management server must be a member of the domain that your mobilEcho file servers reside on. Users will authenticate to the management server with their Active Directory credentials.

Configuring the Client Management Service

Before the Client Management service is enabled, some fundamental settings must be entered in its configuration file. To access the mobilEcho Client Management configuration file:

1. Ensure that mobilEcho is installed on the Windows server designated as your mobilEcho Client

Management Server.

2. Navigate to the **mobilEcho Server** program folder. The default location is **C:\Program Files\Group Logic\mobilEcho Server** on **32-bit** versions of Windows and **C:\Program Files (x86)\Group Logic\mobilEcho Server** on **64-bit** versions of Windows.
3. Enter the **ManagementUI** folder and open the **mobilEcho_manager.cfg** file a text editor application. If your default language includes Unicode characters, be sure that your text editor is UTF-8 compatible and saves the config file in UTF-8 format.

The **mobilEcho_manager.cfg** file contains the base settings that mobilEcho Client Management requires to function. Detailed instructions are included in the file. Required settings include:

HTTPS_PORT

The mobilEcho Client Management Server UI uses port 3000 for HTTPS web browser access by default. This port can be changed to anything you like. A change to this setting requires a restart of the **mobilEcho Management** service to take effect.

MANAGEMENT_SESSION_TIMEOUT

The number of minutes the mobilEcho Client Management Administrator can be idle before a session is terminated and the administrator is required to log in again.

HTTPS_USE_AUTOGENERATED_CERTS

This setting defaults to **true**. When set to **true** mobilEcho will generate a self-signed SSL certificate. This will allow network access to the mobilEcho Client Management web UI to be encrypted, but will produce a warning in most web browsers. If you would like to obtain, or already have, a third-party issued SSL certificate for this server, you can change this setting to **false** and enter the paths to your key and certificate in the related settings below. A change to this setting requires a restart of the **mobilEcho Management** service to take effect.

> **Firefox Incompatibility**
>
> In Firefox, auto-generated certificates can often result in an error regarding a duplicate certificate serial number. It is recommended you do not use Firefox to access servers using auto-generated certificates.

HTTPS_KEY

Enter the path on disk to your certificate's key. A change to this setting requires a restart of the **mobilEcho Management** service to take effect.

HTTPS_CERT

Enter the path on disk to your certificate. A change to this setting requires a restart of the **mobilEcho Management** service to take effect.

MANAGEMENT_SERVER_ADDRESS

Enter the DNS name or IP address of this management server. This information is used to create the client management invitation file that instructs your mobilEcho clients where to access the management server.

It is possible to configure your mobilEcho file servers to require that a client is managed by a particular mobilEcho management server, ensuring that all clients have the proper application and security settings in place before they gain access. In order for this feature to work, the address used by the client must match the address allowed on the server. Therefore, it is important that you use a consistant DNS name or IP address on all mobilEcho clients so they access the mobilEcho management server using the same address.

It is recommended that you create a unique DNS name for your management server that can be reconfigured to point to any server you may decide to move the management server role to in the future.

VALID_LOGIN_NAMES

The mobilEcho Client Management Administrator authenticates users with Active Directory at login. For this setting, provide a comma separated list of the usernames or Active Directory groups that you would like to be allowed to log into the administrator web UI. This setting simply serves as an allow list. The username and password entered will always be verified with Active Directory before a user can successfully log in.

LDAP_HOST

Enter the DNS name or IP address of the Active Directory server you would like mobilEcho Client Management to use for regulating access to the web UI and for setting up your user and group profiles.

LDAP_PORT

The default Active Directory port is 389. This will likely not need to be modified.

LDAP_IS_SSL

The default is **no**. Change this setting to **yes** to connect to Active Directory using secure LDAP.

LDAP_DOMAIN

Enter your domain name. As an example, GroupLogic's full domain name is *grouplogic.com*. For this setting, just the base domain name *grouplogic* is entered.

LDAP_SEARCHBASE

Enter the root level you would like searches for users and groups to be assigned mobilEcho profiles to begin. If you would like to search your entire domain, enter "dc=domainname, dc=domainsuffix". For the GroupLogic example, this would be: dc=grouplogic, dc=com

SMTP_SERVER_ADDRESS

Enter the DNS name of an SMTP server that will be used to send client management enrollment email invitations to your users. This is required to add devices to the mobilEcho management server.

SMTP_SERVER_PORT

Enter your SMTP server port. This setting defaults to port 587.

SMTP_USE_SECURE

Enable or disable the option to use a secure SSL connection to your SMTP server. This setting defaults to

false. Set this to **true** to enable secure SMTP.

SMTP_USERNAME

If required by your SMTP server, enter a username for SMTP authentication. Leave this blank if no authentication is required.

SMTP_PASSWORD

If required by your SMTP server, enter a password for SMTP authentication. Leave this blank if no authentication is required.

SMTP_FROM_NAME

Enter the name that users will see as the From name when they receive an enrollment invitation email.

SMTP_FROM_ADDRESS

Enter the email address that users will see as the From address when they receive an enrollment invitation email.

SMTP_EMAIL_SUBJECT

Enter the Email Subject that users will see when they receive an enrollment invitation email.

DEFAULT_INVITATION_TIMEOUT

Enter the default number of days you would like an enrollment PIN number to be valid before it expires.

```
###
# Management web server port
#
# The port the management server listens on.
# You must restart the server for changes to be applied.

HTTPS_PORT = 3000

###
# Management session timeout
#
# The number of minutes a management session may be idle before the session is terminated
# and the administrator must log in again.

MANAGEMENT_SESSION_TIMEOUT = 15

###
# Management server security settings
#
# If you set HTTPS_USE_AUTOGENERATED_CERTS to true (the default), the web server will
# generate its own certificate to run securely.  This auto-generated certificate will
# ensure that the connection is encrypted, but because it is not certified by a certificate
# authority, it may cause warnings in the client's browser.
#
# In Firefox, auto-generated certificates can often result in an error regarding a duplicate
# certificate serial number. It is recommended you do not use Firefox with servers using
# auto-generated certificates.
#
# To use a certificate obtained from a certificate authority, set HTTPS_USE_AUTOGENERATED_CERTS
# to false and set HTTPS_KEY and HTTPS_CERT to the paths to that key and certificate.
#
# You must restart the server for changes to be applied.

HTTPS_USE_AUTOGENERATED_CERTS = true

HTTPS_KEY = path/to/keyfile.key
HTTPS_CERT = path/to/certificate.crt

###
# Server information
#
# This information is used when sending management enrollment invitation emails to users.
# Specify the DNS name or IP address of the server hosting the management server.
# Clients will use this address to contact the management server on an ongoing basis.
# It is best to set this to a unique DNS address created for the management server.
# If you later decide to move the management server role to a different server, simply updating
# the DNS record will point all existing clients to the new server.
#
# Changes will applied immediately; no server restart is required.

MANAGEMENT_SERVER_ADDRESS = example.server.com

###
# Authentication Settings
#
# Provide a comma-separated list of valid login names that are permitted to log in to administer
# the management server.  Note that these valid login names are only used to determine which
# accounts have access to the mobilEcho Client Management Administrator. The username / password
# combination will then be authenticated against AD before the user can successfully log in.
#
# Valid login names may be user or group names.  If groups are listed, any members of those
# groups or subgroups can log in to the management server, provided AD authenticated is
# successful.  The user's primary group (usually "Domain Users") cannot be used.
#
# Changes will applied immediately; no server restart is required.

VALID_LOGIN_NAMES = example1, example2

###
# LDAP / Active Directory Settings
#
# Changes will applied immediately; no server restart is required.

# Enter the DNS name or IP address of your Active Directory server.
LDAP_HOST = ldap.example.com

# Enter the LDAP port and whether or not it is an SSL port ("yes" or "no").  Typically, LDAP port
# 389 (LDAP), 3268 (global catalog), 636 (LDAP over SSL) and 3269 (global catalog over SSL)
LDAP_PORT = 389
LDAP_IS_SSL = no

# Enter the name of your domain and the search base. Do not add the domain suffix to the domain
# field. If your domain is 'example.com', enter only "example" in the LDAP_DOMAIN field. If
# you're not sure what to use as your search base, you can use "dc=domainname, dc=domainsuffix"
# to search your whole domain.

LDAP_DOMAIN = example
LDAP_SEARCHBASE = dc=example, dc=com

###
# SMTP settings
#
# This SMTP server is used to email management enrollment invitations to users.
#
# A restart of the 'mobilEcho Management' service or a server restart is required to apply
```

```
# A restart of the "mobilEcho Management" service or a server restart is required to apply
# changes to any SMTP settings.

SMTP_SERVER_ADDRESS  = smtp.example.com
SMTP_SERVER_PORT  = 587
SMTP_USE_SECURE  = false

# If you do not require SMTP authentication, you can
# leave SMTP_USERNAME and SMTP_PASSWORD blank.
SMTP_USERNAME  =
SMTP_PASSWORD  =

# Name and email address that invitations will be from
SMTP_FROM_NAME   = mobilEcho Invitation
SMTP_FROM_ADDRESS  = mobilEcho_invitation@example.com

# Email subject of the invitation
SMTP_EMAIL_SUBJECT = Welcome to mobilEcho

###
# Enrollment Settings
#
# Settings related to management enrollment

# Default time (in days) that management invitations are valid before the one-time PINs expire
DEFAULT_INVITATION_TIMEOUT = 5
```

Save the configuration file

Once these options have been configured, save the **mobilEcho_manager.cfg** file.

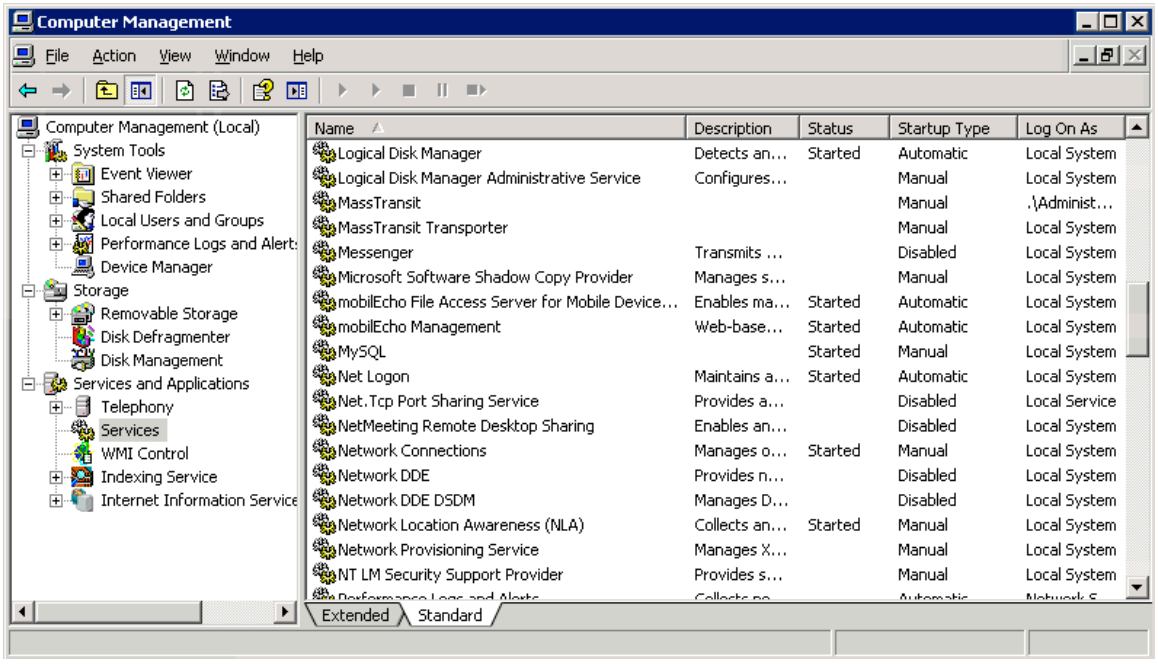
These settings can later be confirmed from the mobilEcho Client Management Administrator's **Settings** p age.

Enabling the mobilEcho Management Service

mobilEcho Client Management runs as a standard Windows service. This service is disabled by default. To enable the mobilEcho Management service:

1. Open the Windows **Start** menu
2. Right click on **My Computer** and select **Manage** to open the **Computer Management** console
3. Under the **Services and Applications** section, select **Services**
4. Scroll down to the **mobilEcho Management** service
5. Right click **mobilEcho Management** and select **Properties**
6. Change **Startup type** to **Automatic**
7. Click the **Start** button
8. Click **OK** to close the **Properties** dialog
9. Confirm that the **mobilEcho Management** service is listed as **Started** and close the **Computer Management** console

The mobilEcho Management service is now started and will start up automatically any time your server is rebooted.



Configuring mobilEcho Client Management Profiles

Once the mobilEcho Management service is started, you can proceed to log in and configure your management settings.

Logging In

The mobilEcho Client Management Administrator is accessed through a web browser. This will always work when using a browser running on the actual management server. Note again that Firefox is not recommended if you are using the default automatically generated self-signed SSL certificate on your server.

Firewall Requirements

If you would like to access the mobilEcho web interface from another computer, you will need to ensure that there is an exception configured for the mobilEcho web interface in the Windows Firewall service.

The default HTTPS port used by the mobilEcho Client Management Administrator is port 3000. It is recommended that you configure a generic, port-specific firewall exception for this port.

mobilEcho URL

To connect to the mobilEcho web interface, enter this URL in your browser. Note that you must start the URL with https://

- https://servername:3000

If you have modified the default port, you will need to use the new value instead of 3000.

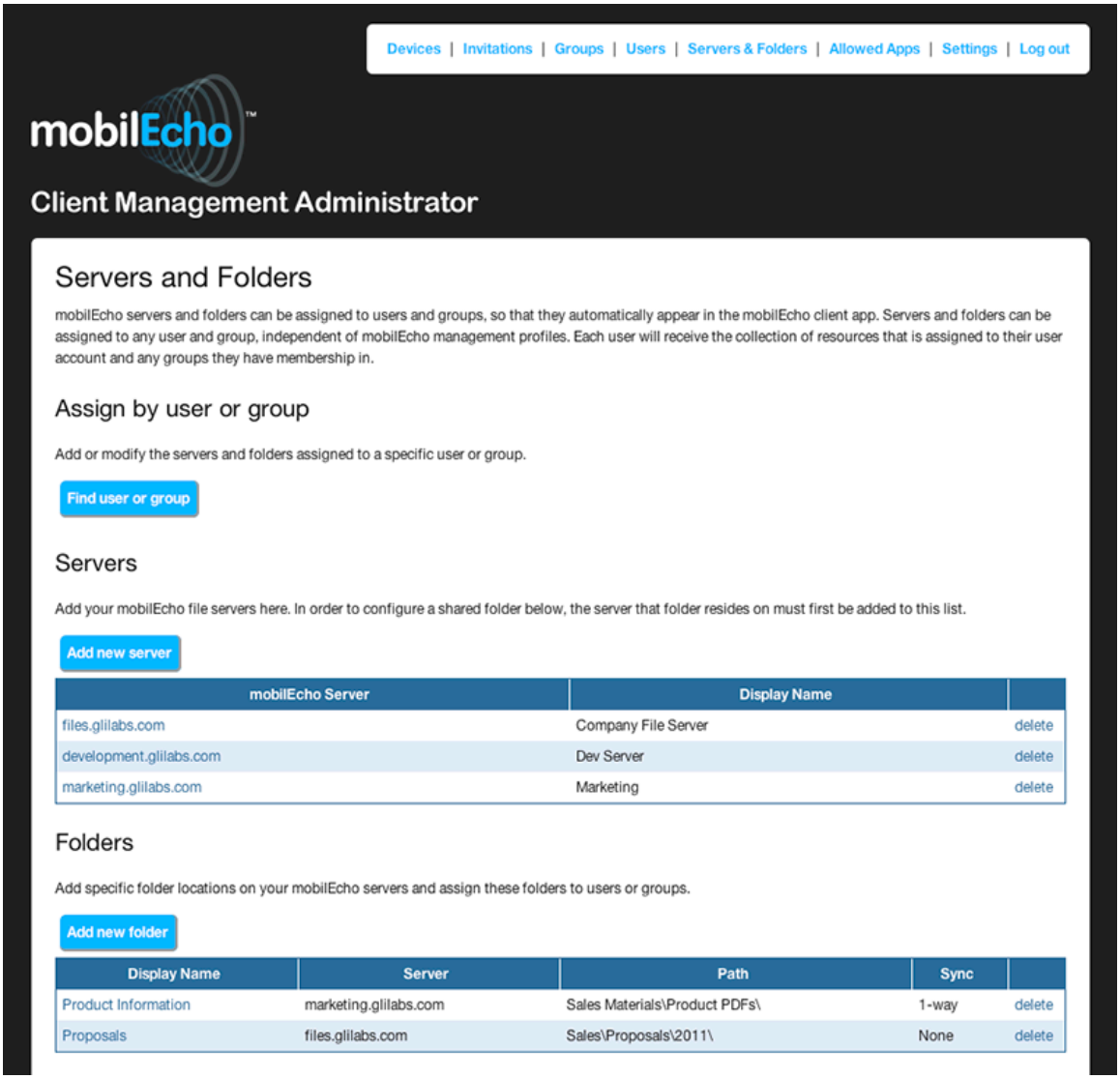
Log In

The initial page you will see is the **Log in** page. You may log in with any account that was included in the **VALID_LOGIN_NAMES** setting in the **mobilEcho_manager.cfg** config file. Enter your Active Directory username and password.

If you have trouble logging in, confirm that your LDAP settings are valid in the **mobilEcho_manager.cfg** config file.

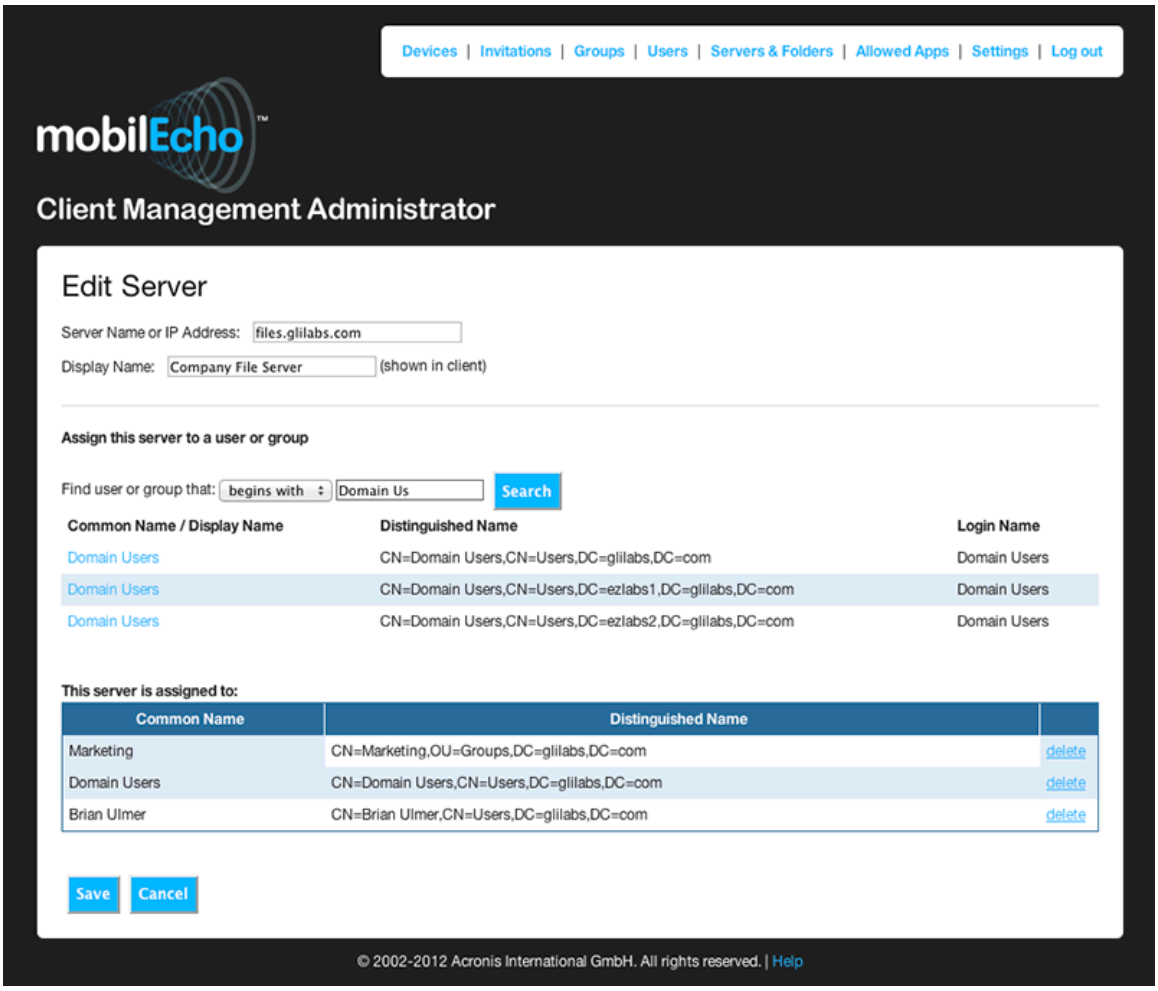
Entering your mobilEcho File Server names

The mobilEcho Client Management Server needs to know about the mobilEcho File Servers on your network. You will need to configure this list of servers before setting up profiles. You can also configure these servers to to automatically appear in the user's mobilEcho client application. Any Active Directory user or group can be assigned a mobilEcho server. The user will then be able to access any mobilEcho volumes on that server that their AD user account has permission to access.



Adding a Server

1. Click **Servers & Folders** in the top menu.
2. Click the **Add new server** button.
3. Enter the **Server Name or IP Address** that you would like clients to use to connect to the server.
4. Enter a **Display Name**. This name will be shown in the mobilEcho client application to identify the server.
5. Optionally, search for an Active Directory User and Group you'd like to assign this new server to, and click the user or group name. This will result in the server automatically appearing in that user's or group's mobilEcho app.
6. Click the **Save** button.



Adding an Assignable Folder

In addition to Servers, Folders can also be assigned to mobilEcho user and group profiles, allowing them to automatically appear in a user's mobilEcho client application. Folders can be configured to point to any mobilEcho shared volume, or even a subdirectory within a shared volume. This allows you to give a user direct access to any folders that might be important to them. By doing so, they don't have to navigate to the folder by knowing the exact server, shared volume name, and path to the folder.

Folders can point to any type of content that mobilEcho is providing access to. They simply refer to locations in mobilEcho volumes that have already been configured within the mobilEcho Administrator. This can be a local file share volume, a "network reshare" volume providing access to files on another file server or NAS, or a SharePoint volume.

Folders can optionally be configured to sync to the client device. mobilEcho folder sync options include:

- **None** - The folder will appear as a network-based resource in the mobilEcho client app and can be accessed and worked with just like a mobilEcho server.
- **1-Way** - The folder will appear as a local folder in the mobilEcho client app. Its complete contents will be synced from the server to the device and it will be kept up to date if files on the server are added, modified, or deleted. This folder is intended to give local/offline access to a set of server-based files and appears as read-only to the user.
- **2-Way** - The folder will appear as a local folder in the mobilEcho client app. Its complete contents will initially be synced from the server to the device. If files in this folder are added, modified, or deleted, either on the device or on the server, these changes will be synced back to the server or device.

Android clients do not support sync folders

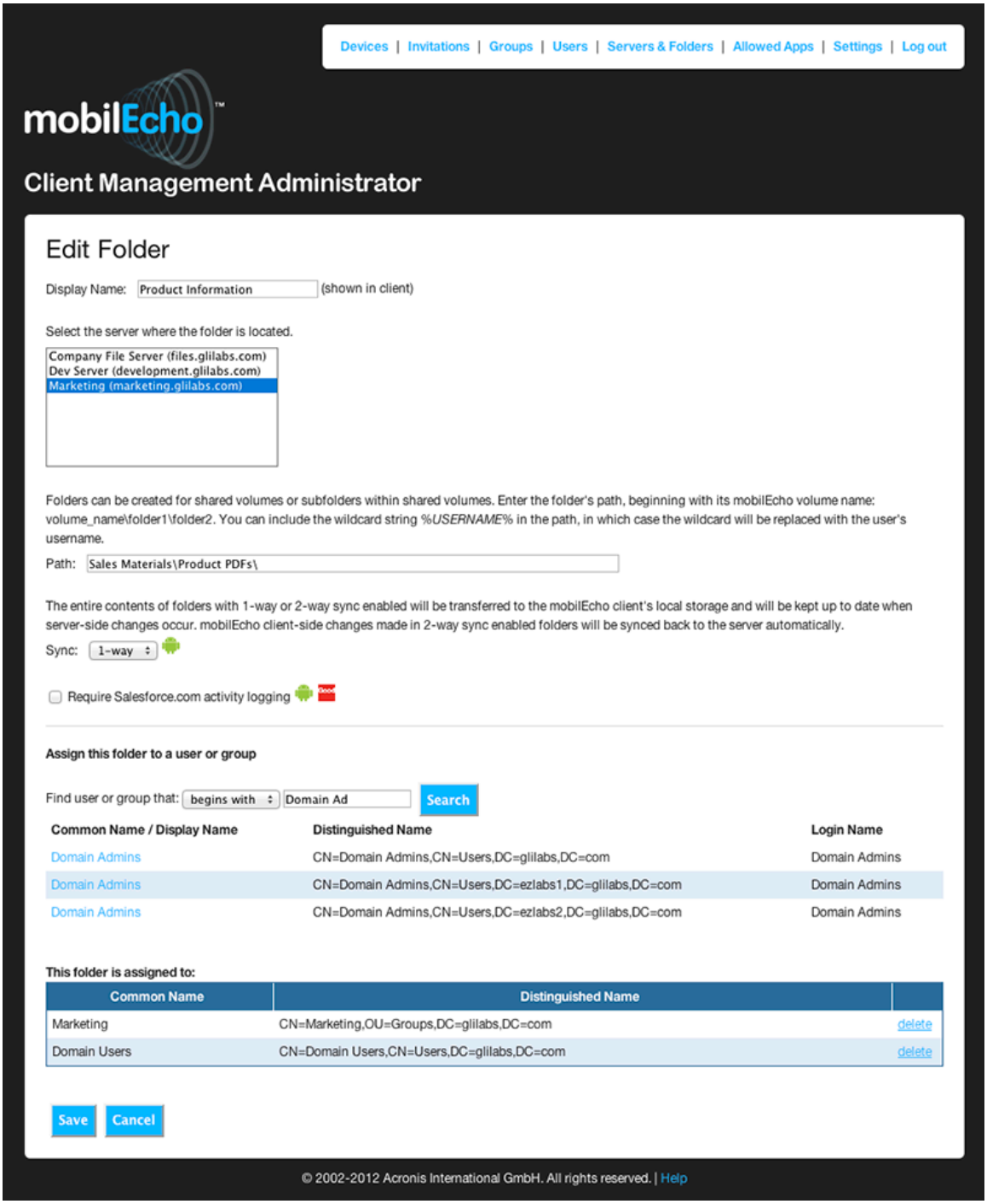
The current version of the mobilEcho for Android app does not support the synchronization of folders. Any assigned folders that are configured as 1-Way or 2-Way sync folders will appear as standard, unsynced network folders on Android devices. Support for sync folders will be added in a future release of mobilEcho for Android.

Require Salesforce activity logging

- GroupLogic has partnered with Salesforce to offer an option for logging access to files shown to customers using mobilEcho. Enabling this option will require any user who has this folder assigned to their mobilEcho management profile to log a customer activity in Saleforce before they can open any file in the folder. This is done completely within the mobilEcho client app.
- All items in this folder will be restricted from being emailed, printed, copied or moved outside this folder, or opened in other apps on the device.
- This feature requires a mobilEcho client and server of version 3.1 or later.
- mobilEcho for iOS clients earlier than version 3.1 and mobilEcho for Android clients will not receive these restrictions. If you need to ensure that all clients accessing this folder are on 3.1 or later. You can set the minimum client version setting on the server the folder resides on to: 3.1.0.133 Details can be found in this knowledge base article: Setting the minimum allowed mobilEcho client version on a mobilEcho server

To add a folder:

1. Click **Servers & Folders** in the top menu.
2. Click the **Add new folder** button.
3. Enter a **Display Name**. This name will be shown in the mobilEcho client application to identify the server.
4. Select the mobilEcho server that contains the mobilEcho volume where the folder is located. If the server is not listed, you must first add it to the **Servers** list on the **Servers & Folders** page.
5. Enter the folder's **Path**. The path must begin with the mobilEcho shared volume name. If the path of the folder specific doesn't start with a mobilEcho volume name, the folder will not function when users try to access it. If you would like to give access to a subfolder in that shared volume, include the full path to that subfolder in the **Path** field.
    - You can include the wildcard string %USERNAME% in the path. This wildcard will be replaced with the user's account username.
    - SharePoint sites and document libraries are displayed when browsing in the mobilEcho app using their "Title". It is possible for a site's title to be different from the site's URL name. For example, http://sharepoint.company.com/testsite might have a title of "Test Site". You may use either the URL path or the Title when configuring Folders that point to SharePoint locations. The entire path that you specify must use either the titles or URL names of any sites, subsites, and document libraries referenced in the path.
6. Choose a **Sync** option. **None**, **1-way**, or **2-way**. See above for details on each option.
7. Optionally, enable **Require Salesforce activity logging**.
8. Search for an Active Directory User and Group you'd like to assign this new folder to, and click the user or group name. This will result in the folder automatically appearing in that user's or group's mobilEcho app.
9. Click the **Save** button.



Adding a Network Reshare Path Mapping

mobilEcho includes a 'Network Reshare' feature, that allows a mobilEcho server to host a shared volume that gives access to data located on a second file server. The mobilEcho server uses the SMB/CIFS protocol to connect to the secondary file server.

mobilEcho also includes the ability to automatically show a user's Active Directory assigned home folder in the mobilEcho client app. These home directory locations are specified by SMB path in the user's Active Directory user account profile.

Warning:

The shared volume name is case sensitive. If the case sensitivity is not followed in the SMB path, you will receive a "The share is unavailable." message when trying to access the home folder in your mobilEcho client.
If you have already received that error, but still keep seeing it after correcting the issue, it is possible that the old SMB path has remained cached in the mobilEcho client. The fastest way for the changes to take effect would be to change the display name of the home folder.

If mobilEcho is installed directly on the server hosting your users' Active Directory assigned SMB home folders, and a mobilEcho shared volume has been created with the same name and location as the SMB home folders shared volume, the mobilEcho UNC path to the home folders shared volume will be identical to the UNC path to the SMB home folders shared volume, and the UNC path specified in the user's Active Directory profile home folder setting will be correct for both SMB access and mobilEcho access.

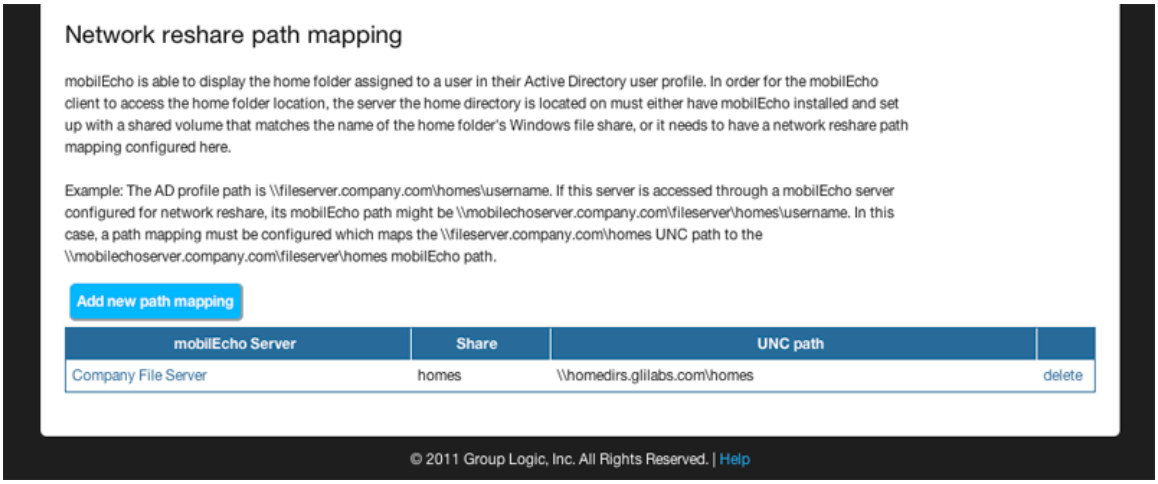
If you are using mobilEcho's Network Reshare feature to give access to home directories on a secondary SMB file server, the SMB UNC path in a user's Active Directory profile home folder setting will not match the mobilEcho UNC path, since mobilEcho servers access their home folders by connecting to a different server.

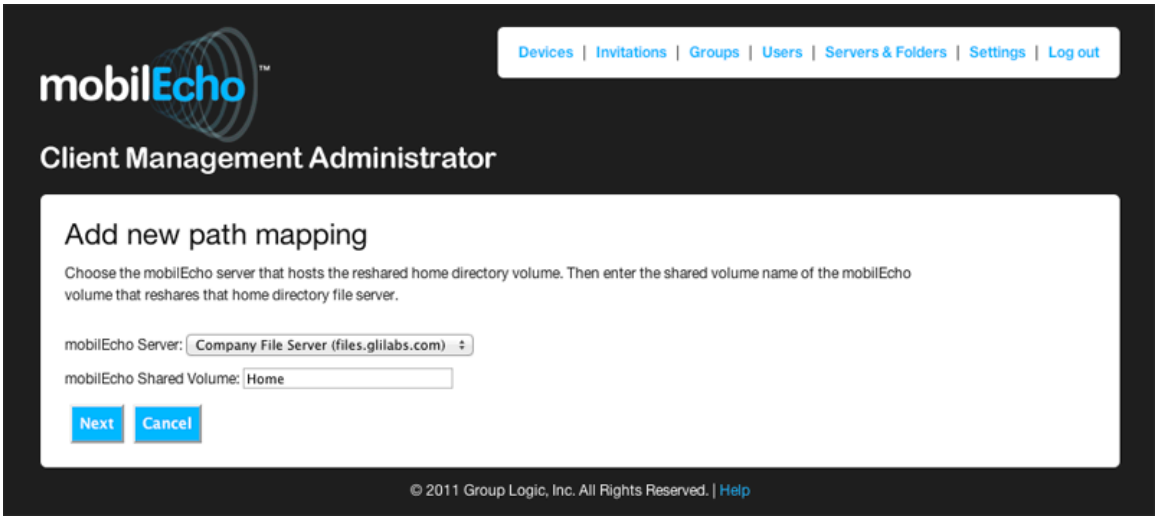
In this case, you will need to configure a Network Reshare Path Mapping, so that mobilEcho knows how to translate the SMB UNC path it gets from the Active Directory profile home folder setting to the mobilEcho UNC path that the mobilEcho client needs to know to connect to the home folder.

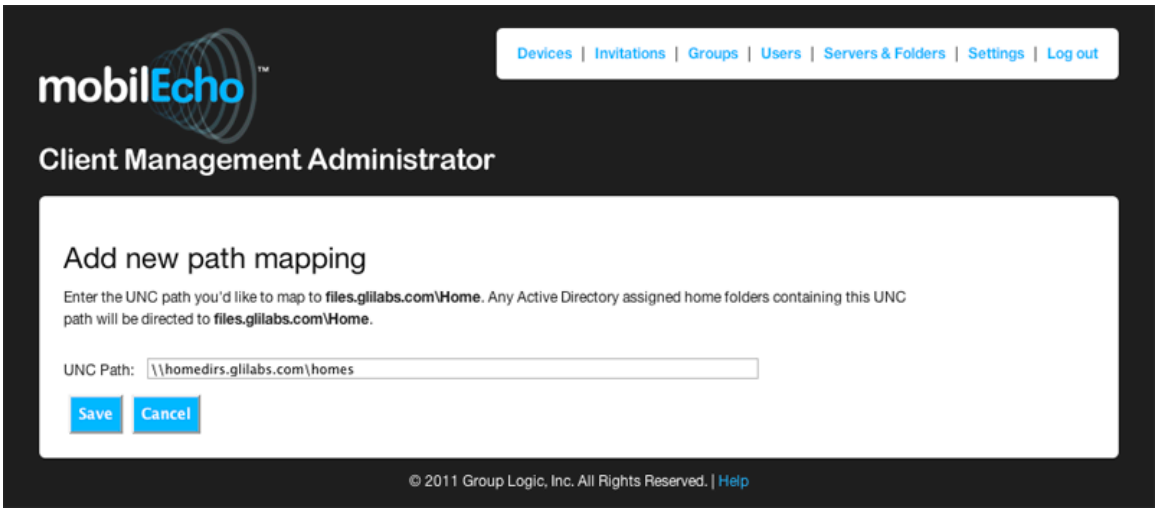
1. Click **Servers & Folders** in the top menu.
2. Click the **Add new path mapping** button.
3. Select the **mobilEcho server** where the mobilEcho network reshare shared volume is located. Then enter the name of the **mobilEcho Shared Volume** (case sensitive).
4. Click **Next**.
5. Enter the **UNC Path** that you would like to be redirected to the mobilEcho Shared Volume you specified in the previous step.
6. **Important Note:** Because mobilEcho is matching on this path, the **UNC Path** needs to use the exact server name and SMB shared volume name as it appears in your users' Active Directory user profile home folder setting. If an SMB home folder's path in Active Directory uses a different name for the server than is entered in the path mapping setting (such as "\\fileserver.company.com\sharename" vs. "\\fileserver\sharename") the home directory will not work in the mobilEcho client. If you've used more than one method for representing your server's name in the Active Directory profile home folder setting for your users, you will need to create a path mapping for each variation on the server name.
7. Click the **Save** button.

Home Directory support when mobilEcho server is running on a non-default port

mobilEcho clients connect to mobilEcho servers on port 443 by default. If the mobilEcho server that contains your home directory shared volume is configured to use a different port, you will need to create a **Network reshare path mapping** that points to the correct mobilEcho server and share on the correct port, so that the mobilEcho client will know to connect to the server on the non-default port. This will be necessary, even if your home directory share is located directly on local storage on your mobilEcho server. In this case a path mapping is necessary to translate an AD home directory SMB path like "\\fileserver.company.com\sharename" to the correct mobilEcho path "\\fileserver.company.com:444\sharename". The correct port just needs to be appended to the server's name or IP address when you add the server to the mobilEcho Client Management server list.







Deleting a Server, Folder, or Network Reshare Path Mapping

Servers, folders, and network reshare path mappings can be deleted from the **Servers & Folders** lists by clicking **delete**. When servers or folders are deleted, they are removed from any profiles they are assigned to.

Creating a Third Party App Whitelist or Blacklist

mobilEcho Client Management allows you to create whitelists or blacklists that restrict mobilEcho's ability to open files into other apps on a mobile device. These can be used to ensure that any files accessible through the mobilEcho client can only be opened into secure, trusted apps.

Whitelists - allow you to specify a list of apps that mobilEcho files are allowed to be opened into. All other apps are denied access.

Blacklists - allow you to specify a list of apps that mobilEcho files are not allowed to be opened into. All other apps are allowed access.

In order for mobilEcho to identify a particular app, it needs to know the app's **Bundle Identifier**. A list of common apps, and their bundle identifiers, are included in the mobilEcho Client Management Administrator by default. If the app you need to whilelist or blacklist is not included, you will need to add it to the list.

> **App whitelisting / blacklisting is not supported on Android**
>
> The mobilEcho for Android client does not currently support whitelisting or blacklisting the 3rd party apps that users are allowed to open files into. This support will be added in a future release. It is possible to fully disable opening files into 3rd party Android apps from within a mobilEcho client management policy.

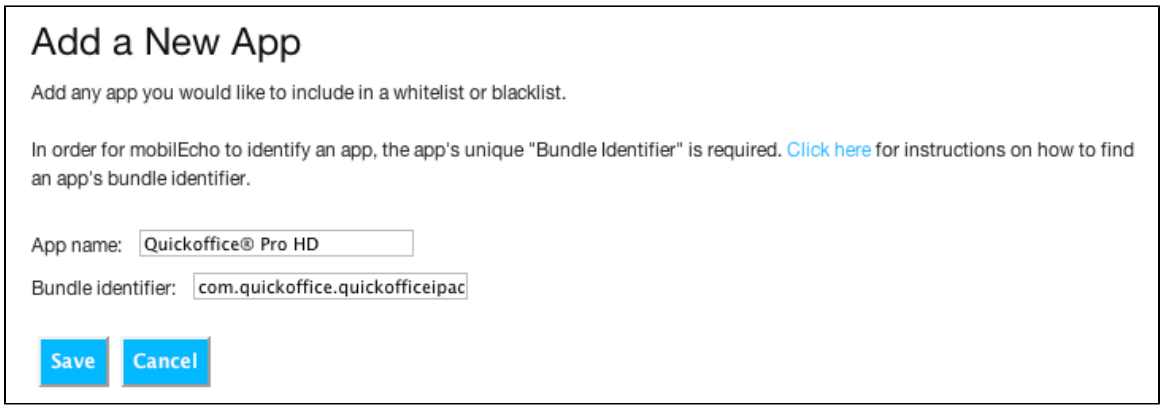
Adding Apps

To add an app to be included on a whitelist or blacklist:

1. Click **Allowed Apps** in the top menu bar.
2. Click **Add app** in the **Apps Available for Lists** section.
3. Enter the **App name**. This can be the name of the app as it appears in the App Store, or an alternate name of your choosing.

4. Enter the app's **Bundle identifier**. This must match the intended apps bundle identifier exactly, or it will not white or blacklisted.
5. Click **Save**.

There is unfortunately no way to look these **Bundle Identifiers** up in the App Store or elsewhere at this time. To find a bundle identifier, you will need to look at a file inside the app.



Finding an app's bundle identifier in an iTunes Library

If you sync your device with iTunes and the app you desire is either on your device, or was downloaded through iTunes, it will exist on your computer's hard drive. You can locate it on your hard drive and look inside the app to find the **bundle identifier**.

1. Navigate to your iTunes Library and open the **Mobile Applications**folder.
    a. On a Mac, this is typically in your home directory, in ~/Music/iTunes/Mobile Applications/
    b. On a Windows 7 PC, this is typically in C:\Users\username\My Music\iTunes\Mobile Applications/
2. If you have recently installed the app on your device, make sure you have performed an iTunes sync before you continue.
3. Locate the app that you require in the **Mobile Applications** folder.
4. Duplicate the file and rename the extension to .ZIP
5. Unzip this newly created ZIP file and you'll end up with a folder with the application name.
6. Inside that folder is a file called **iTunesMetadata.plist**
7. Open this PLIST file in a text editor.
8. Find the **softwareVersionBundleId** key in the list.
9. The **string** value below it is the bundle identifier value that you will need to enter for the app in mobilEcho. These are commonly formatted as: **com.companyname.appname**

Finding an app's bundle identifier by browsing the files on your device

If you use software that allows browsing the contents of your device's storage, you can locate a app on the device and determine its **bundle identifier**. One app that can be used for this is iExplorer.

1. Connect your device to your computer with USB and open iExplorer or a similar utility.
2. Open the Apps folder on the device and locate the app you require.
3. Open that app's folder and locate its **iTunesMetadata.plist** file.
4. Open this PLIST file in a text editor.
5. Find the **softwareVersionBundleId** key in the list.
6. The **string** value below it is the bundle identifier value that you will need to enter for the app in mobilEcho. These are commonly formatted as: **com.companyname.appname**

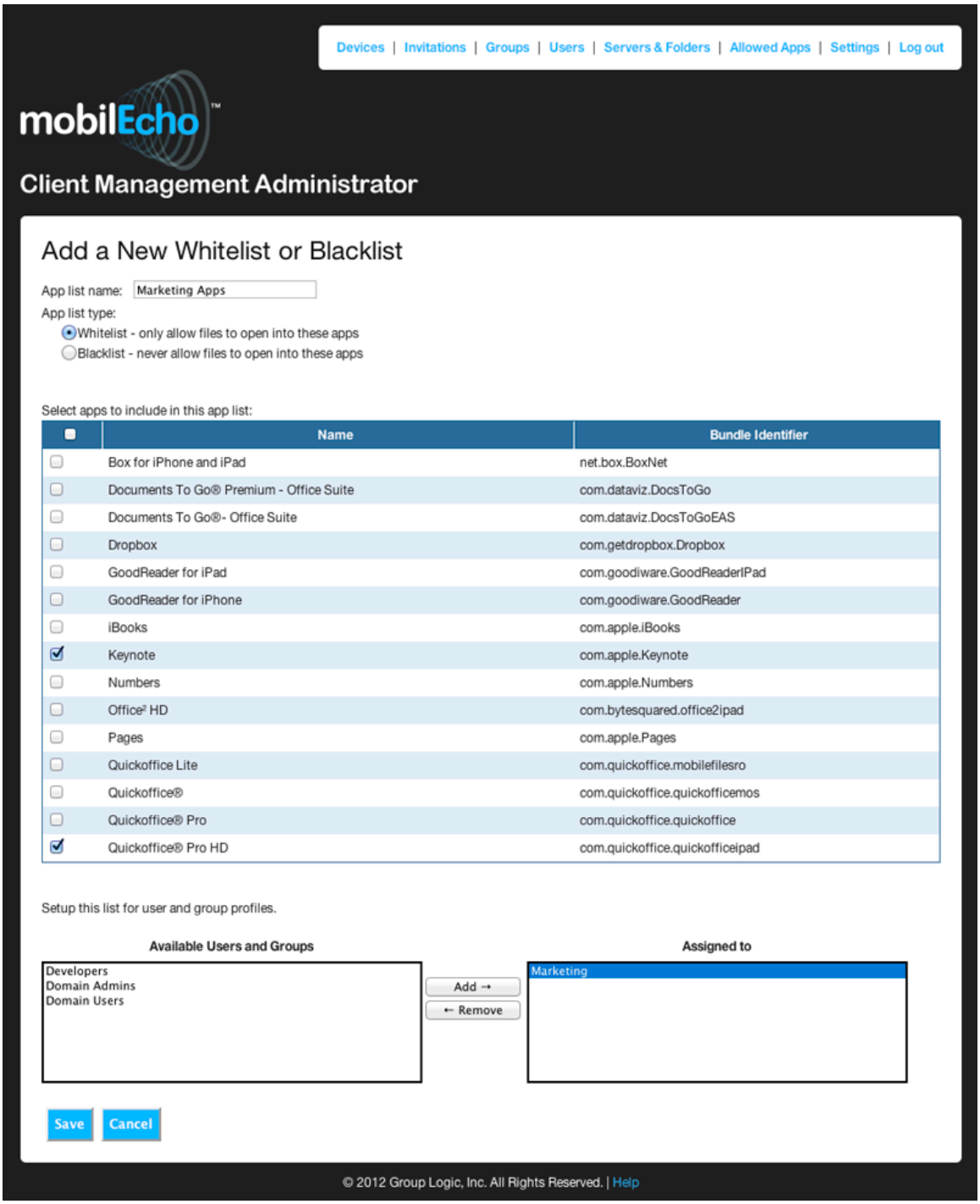
Creating a whitelist or blacklist

mobilEcho allows you to create any number of app whitelists or blacklist. Because whitelists inherently allow no apps by default, and blacklists inherently allow all apps by default, mobilEcho only allows one whitelist or blacklist to be assigned to a mobilEcho user or group profile.

To create a new list:

1. Click **Allowed Apps** in the top menu bar.
2. Click **Add list** in the **Lists** section.
3. In **App list name**, give your list a descriptive name of your choosing.
4. Select the type of list you would like to create, **Whitelist** or **Blacklist**.
5. Select the checkbox next to each app you would like to include in the list.
6. If you would like to go ahead and assign this new list to any existing user or group profiles, select them in the **Available Users and Groups** list and click **Add**.
7. Click **Save**.

Whitelists and blacklists can also be assigned to profiles within the profiles configuration page. This process is detailed in the next section of this guide, Managing Group Profiles.



Managing Group Profiles

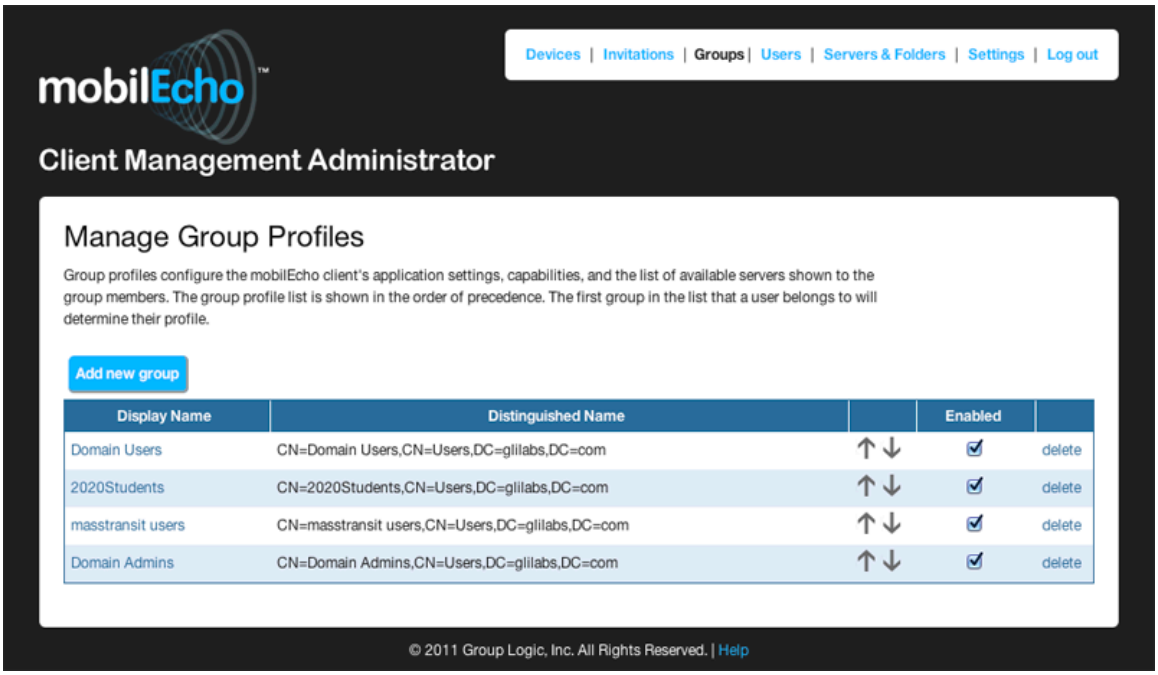
mobilEcho Client Management allows profiles to be assigned to Active Directory groups. Group profiles will usually address most or all of your client management requirements. The group profiles list is displayed in order of precedence, with the first group in the list having the highest priority. When a user contacts the mobilEcho management server, their settings are determined by the single highest priority group profile they are a member of.

Group Management Tips

If you would like all or most of your users to receive the same profile settings, you can set up a profile for the **Domain Users** group and place it at the bottom of the prioritized list. Any groups that need special profiles can be created and prioritized above the **Domain Users** group.

If you would like to deny a group of users access to mobilEcho management, ensure that they are not members of any configured group profiles. As long as a user account does not match any group profiles, they will be denied the ability to enroll in mobilEcho client management.

To access the group profiles list, click the **Groups** option in the top menu.



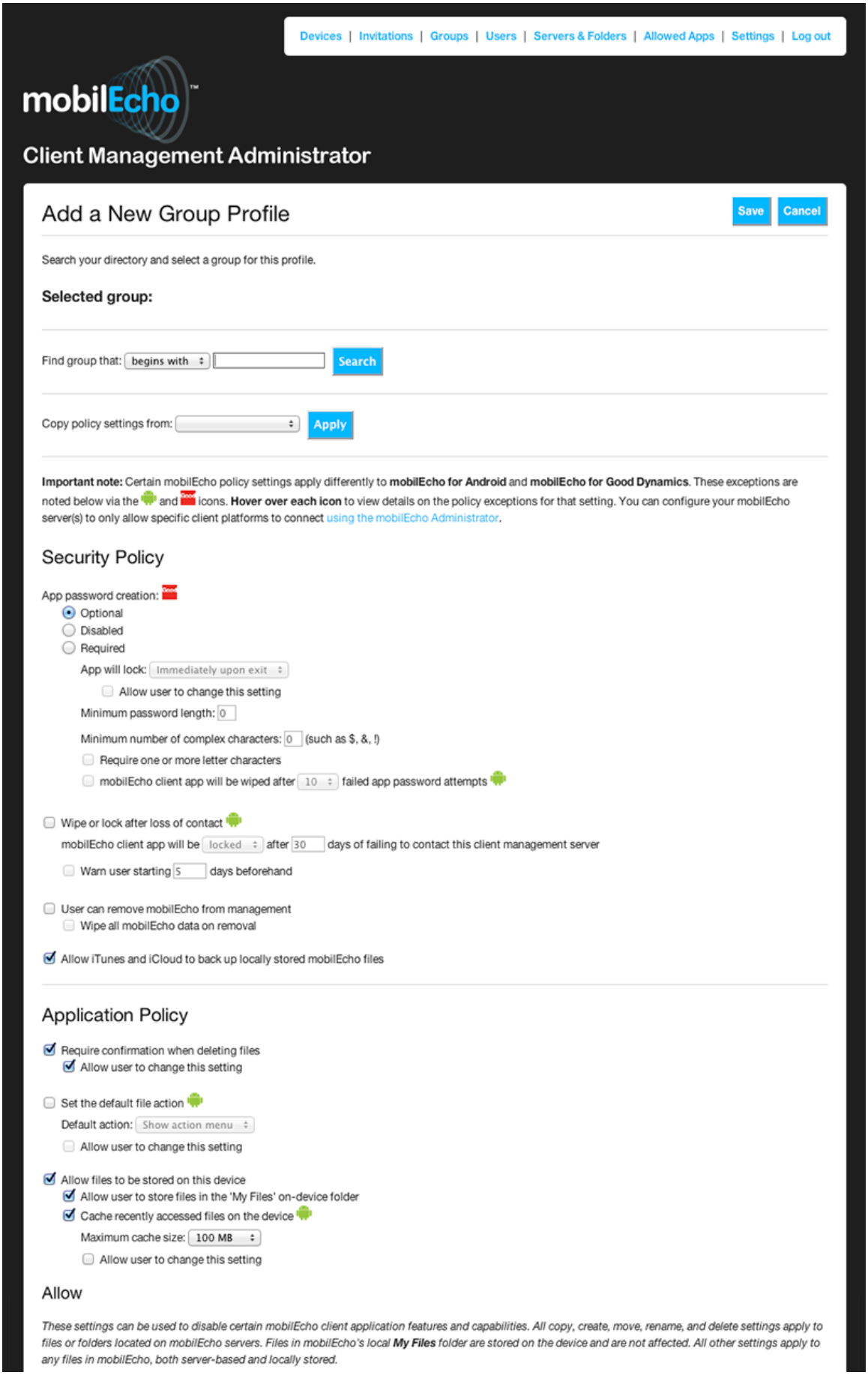
Modifying Group Priority

To change a group's priority, click the up or down arrow in the Manage Groups Profiles list. This will move the profile up or down one level.

Adding a New Group

To add a new group:

1. Click the **Add new group** button to add a new group. This will open the **Add a new group profile** page.
2. In the **Find group** field, enter the partial or complete Active Directory group name for which you'd like to create a profile. You can perform '**begins with**' or '**contains**' searches for Active Directory groups. Begins with search will complete much faster than contains searches.
3. Click **Search** and then find and click the group name in the listed results.




File copies / creation
Folder copies
Opening mobilEcho files in other applications
File deletes
Folder deletes
App whitelist/blacklist: None
File moves
Folder moves
Sending files to mobilEcho from other apps
File renames
Folder renames
Sending files to mobilEcho using Quickoffice 'Save Back'
Adding new folders
Emailing files from mobilEcho
Bookmarking folders
Printing files from mobilEcho
Copying text from previewed files
Allow PDF annotation
User created sync folders
Emailing mobilEcho file links
Opening mobilEcho file links
Server Policy
Required login frequency for resources assigned by this profile:
Once only, then save for future sessions
Once per session
For every connection
Allow user to add individual servers
Allow saved passwords for user configured servers
Only allow this mobilEcho client to connect to servers with third-party signed SSL certificates
Warn client when connecting to servers with untrusted SSL certificates
Client timeout for unresponsive servers: 30 sec
Allow user to change this setting
Synced Folder Settings:
Client is prompted to confirm before synced files are downloaded: Always
Only allow file syncing while device is on WiFi networks
Resource Assignment
Select the folders and servers that will automatically appear in the mobilEcho client application.
Display the user's home folder
Display name shown on client: Home Folder
Home directory type:
Active Directory assigned home folder
Custom home directory path: Company File Server (files.glilabs.com)
The mobilEcho servers and folders assigned to Active Directory users and groups are now configured exclusively on the Servers & Folders page. You may assign any number of users or groups to each of these resources.
Save
Cancel
© 2012 GroupLogic, Inc. All Rights Reserved. | Help

Exceptions for policy settings for Android and Good Dynamics

For users running the **mobilEcho for Android** and **mobilEcho for Good Dynamics** (iOS) apps, there are some exceptions to the way mobilEcho client management policies are applied to the mobilEcho client app. In the case of Android, a few of the features of the iOS client are not yet supported, so the related policies do not apply. In the case of Good Dynamics, a few of the standard mobilEcho policy features are deferred to the Good Dynamics system and the Good Dynamics policy set that you have configured on your Good Control server. These exceptions are noted on the mobilEcho policy configuration pages. Hover over the Good and Android logos for more details on the individual policy exceptions.

The following options can be defined in a group profile:

Security Policy settings

- **App password creation** - The mobilEcho client application can be set with a lock password that must be first entered when launching the application.
    - **Optional** - This setting will not force the user to configure an application lock password, but they will be able to set one from the Settings menu within the app if they desire.
    - **Disabled** - This setting will disabled the ability to configure an application lock password from the Settings menu within the app. This might be useful in the case of shared mobile devices where you prefer that a user cannot set an app password and will lock other users out of mobilEcho.
    - **Required** - This setting will force the user to configure an application lock password if they do not already have one. The optional application password complexity requirements and failed password attempt wipe setting only apply when **App password creation** is set to **Required**.
- **App will lock** - This setting configures the application password grace period. When a user switches from mobilEcho to another application on their device, if they return to mobilEcho before this grace period has elapsed, they will not be required to enter their application lock password. To require that the password is entered every time, choose **Immediately upon exit**. If you would like the user to be able to modify their **App will lock** setting from within the mobilEcho client settings, select **Allow user to change this setting**.
- **Minimum password length** - The minimum allowed length of the application lock password.
- **Minimum number of complex characters** - The minimum number of non-letter, non-number characters required in the application lock password.
- **Require one or more letter characters** - Ensures that there is at least one letter character in the application password.
- **mobilEcho client app will be wiped after X failed app password attempts** - When this option is enabled, the settings and data in the mobilEcho client app will be wiped after the specified number of consecutive failed app password attempts.
- **Wipe or lock after loss of contact**- Enable this setting if you would like the mobilEcho app to automatically wipe or lock in the case that it has not made contact with this mobilEcho Client Management server in a certain number of days. Locked clients will automatically unlock in the event that they later contact the server sucessfully. Wiped clients immediately have all the local files stored in the mobilEcho app deleted, their client management profile removed, and all settings reset to defaults. Wiped clients will have to be re-enrolled in mobilEcho to gain access to mobilEcho servers.
    - **Warn user starting [ ] days beforehand** - The mobilEcho app can optionally warn the user when a 'loss of contact' wipe or lock is going to happen in the near future. This gives them the opportunity to reestablish a network connection that allows the mobilEcho app to contact it's mobilEcho management server and prevent the lock or wipe.
- **User can remove mobilEcho from management** - Enable this setting if you would like your mobilEcho users to be able to uninstall their management profile from within mobilEcho. Doing so will return the

application to full functionality and restore any configuration that was changed by their profile.

- **Wipe all mobilEcho data on removal** - When user removal of profiles is enabled, this option can be selected. If enabled, all data stored locally within the mobilEcho application will be erased if it is removed from management, ensuring that corporate data does not exist on a client not under management controls.
- **Allow iTunes to back up locally stored mobilEcho files** - When this setting is disabled, the mobilEcho client will not allow iTunes to back up its files. This will ensure that no files within mobilEcho's secure on-device storage are copied into iTunes backups.

Application Policy settings

- **Require confirmation when deleting files** - When enabled, the user will be asked for confirmation each time they delete a file. If you would like the user to be able to later modify this setting, select **Allow user to change this setting**.
- **Set the default file action** - This option determines what will happen when a user taps a file in the mobilEcho client application. If this is not set, the client application defaults to **Action Menu**. If you would like the user to be able to later modify this setting, select **Allow user to change this setting**.
- **Allow files to be stored on the device** - This setting is enabled by default. When enabled, files will be permitted to remain on the device, within mobilEcho's sandboxed storage. Individual features that store files locally (*My Files*folder, sync folders, recently accessed file caching) can be enabled or disabled using additional profile settings. If this option is disabled, no files will be stored on the device, ensuring that no corporate data is on the device if it is lost or stolen. If this setting is disabled, the user will not be able to save or sync files for offline use, cache files for improved performance, or send files from other applications to mobilEcho using the "Open In" function.
    - **Allow user to store files in the 'My Files' on-device folder** - If enabled, files can be copied into the 'My Files' folder for offline access and editing. This is a general purpose storage area within mobilEcho's on-device storage sandbox.
    - **Cache recently accessed files on the device** - If enabled, server-based files that have been recently access will be saved in a local cache on the device, for use if they are accessed again and have not changed, providing performance and bandwidth conservation benefits. **Maximum cache size** can be specified and the user can optionally be allowed to change this setting.
- **Allow file copies / creation** - If this option is disabled, the user will not be able to save files from other applications or from the iPad Photos library to a mobilEcho server. They will also be unable to copy or create new files or folders on the mobilEcho server. This setting supersedes any NTFS permissions that client may have that allow file creation.
- **Allow folder copies** - If this option is disabled, the user will not be able to copy folders on or to the mobilEcho server. This setting supersedes any NTFS permissions that client may have that allow folder creation. **File copies / creation** must be enabled for this setting to be enabled.
- **Allow file / folder deletes** - If one of these options is disabled, the user will not be able to delete files or folders from the mobilEcho server. This setting supersedes any NTFS permissions that client may have that allow file or folder deletion.
- **Allow file moves** - If this option is disabled, the user will not be able to move files from one location to another on the mobilEcho server, or from the server to the mobilEcho application's local My Files storage. This setting supersedes any NTFS permissions that client may have that allow file or folder moves.
- **Allow folder moves** - If this option is disabled, the user will not be able to move folders from one location to another on the mobilEcho server, or from the server to the mobilEcho application's local My Files storage. This setting supersedes any NTFS permissions that client may have that allow file or folder moves. **Folder copies** must be enabled for this setting to be enabled.
- **Allow file / folder renames** - If one of these options is disabled, the user will not be able to rename files or folders from the mobilEcho server. This setting supersedes any NTFS permissions that client may have that allow file or folder renames.
- **Allow adding new folders** - If this option is disabled, the user will not be able to create new, empty

folders on the mobilEcho server.

- **Allow bookmarking folders** - If this option is disabled, the user will not be able to bookmark on-device or on-server mobilEcho folders for quick shortcut access.
- **Allow opening mobilEcho files in other applications** - If this option is disabled, the mobilEcho client application will omit the **Open In** button and not allow files in mobilEcho to be opened in other applications. Opening a file in another application results in the file being copied to that application's data storage area and outside of mobilEcho control.
- **App whitelist/blacklist** - Select a predefined whitelist or blacklist that restricts that third party apps that mobilEcho files can be opened into on the device. To create a whitelist or blacklist, click **Allowed Apps** i n the top menu bar.
- **Allow sending files to mobilEcho from apps using 'Open In'** - If this option is disabled, the mobilEcho client application will not accept files sent to it from other applications' **Open In** feature.
- **Allow sending files to mobilEcho using Quickoffice 'Save Back'** - If this option is disabled, the mobilEcho client application will not accept files sent to it from the Quickoffice app's **Save Back** feature.
- **Allow emailing files from mobilEcho** - If this option is disabled, the mobilEcho client application will omit the **Email File** button and not allow files in mobilEcho to be emailed from the application.
- **Allow printing files from mobilEcho** - If this option is disabled, the mobilEcho client application will omit the **Print** button and not allow files in mobilEcho to be printed.
- **Allow copying text from previewed files** - If this option is disabled, the mobilEcho client will not allow the user to select text in previewed documents for copy/paste operations. This will prevent data from being copied into other applications.
- **Allow PDF annotation** - If this option is disabled, the mobilEcho iPad client will not be allowed to annotate PDFs.
- **Allow user created sync folders** - If this option is disabled, users will not be able to manually select mobilEcho network folders to 1-way or 2-way sync to their mobilEcho on-device storage.
- **Allow emailing mobilEcho file links** - If this option is disabled, users will not be able to send mobilEcho:// URLs to mobilEcho files or folders to other mobilEcho users. These links are only functional if opened from a device where the recipient has mobilEcho installed and configured with a server or assigned folder that has access to the link location. The user must also have file/folder-level permission to read the item.
- **Allow opening mobilEcho file links** - If this option is disabled, users will not be allowed to open mobilEcho:// URLs to mobilEcho files or folders.

Server Policy settings

- **Required login frequency for servers assigned by this profile**- sets the frequency that a user must log into the servers that are assigned to them by their profile.
    - **Once only, then save for future sessions** - The user enters their password when they are initially enrolled in management. This password is then saved and used for any file server connections they later initiate.
    - **Once per session** - After launching mobilEcho, the user is required to enter their password at the time they connect to the first server. Until they leave the mobilEcho application, they can then connect to additional servers without having to reenter their password. If they leave mobilEcho for any period of time and then return, they will be required to enter their password again to connect to the first server.
    - **For every connection** - The user is required to enter their password each time they connect to a server.

- **Allow user to add individual servers** - If this option is enabled, users will be able to manually add servers from within the mobilEcho client application, as long as they have the server's DNS name or IP address. If you want the user to only have their profile **Assigned Servers** available, leave this option disabled.
- **Allow saved passwords for user configured servers** - If a user is allowed to add individual servers,

this sub-option determines whether they are allowed to save their password for those server.

- **Only allow this mobilEcho client to connect to servers with third-party signed SSL certificates** - If this option is enabled, the mobilEcho client will only be permitted to connect to servers with third-party signed SSL certificates. *Note:* If the management server does not have a third-party certificate, the client will be unable to reach the management server after it's initial configuration. If you enable this option, ensure you have third-party certificates on all your mobilEcho file servers.
- **Warn client when connecting to servers with untrusted SSL certificates** - If your users are routinely connecting to servers that will be using self-signed certificates, you may choose to disable the client-side warning dialog message they will receive when connecting to these servers.
- **Client timeout for unresponsive servers** - This option sets the client login connection timeout for unresponsive servers. If your clients are on especially slow data connections, or if they rely on a VPN-on-demand solution to first establish a connection before a mobilEcho server is reachable, this timeout can be set to a value greater than the 10 second default.
- **Client is prompted to confirm before synced files are downloaded** - Select the conditions under which the user must confirm before files in synced folders are downloaded. Options are: Always, While on 3G networks only, and Never.
- **Only allow file syncing while device is on WiFi networks** - When this option is enabled, mobilEcho will not allow files to be synced over 3G connections.

Resource Assignment

- **Display the user's home folder**- This option causes a user's personal home directory to appear in the mobilEcho client app.
  - **Display name shown on client** - Sets the display name of the home folder item in the mobilEcho client app.
  - **Active Directory assigned home folder** - The home folder shown in the mobilEcho app will connect the user to the server/folder path defined in their AD account profile.
  - **Custom home directory path** - The home folder shown in the mobilEcho app will connect the user to the server and path defined in this setting. The %USERNAME% wildcard can be used to include the user's username in the home folder path. %USERNAME% must be capitalized.
- **Assigned Servers & Folders** - Beginning with mobilEcho 4.1, server and folder assignment is now performed by selecting the desired Server or Folder on the **Servers & Folders** page and then assigning a user or group directly to that resource. Users will now see the full collection of all servers and folders assigned to their user account and to any groups they are a member of.

After setting the required profile options, click **Save**.

You will be returned to the **Groups** list and may then need to change the newly added group's priority.

Modifying Group Profiles

Existing Group profiles can be modified at any time. Changes to profiles will be applied to the relevant mobilEcho client users the next time they launch mobilEcho.

> **Client management connectivity requirements**
>
> mobilEcho clients must have network access to the management server in order to receive profile updates, remote password resets, and remote wipes. If your client is required to connect to a VPN before they can access mobilEcho file servers, they will also need to VPN before management commands will be accepted.

To modify a group profile:

1. Click the **Groups** option in top menu bar. This opens the **Manage Group Profiles** page.

2. Click the group you would like to modify.
3. Make any changes necessary on the **Edit User** page and click **Save**.

Disabling Group Profiles

To temporarily disable a profile:

1. Click the **Groups** option in top menu bar. This opens the **Manage Group Profiles** page.
2. Uncheck the check box in the **Enabled** column for the desired group.
3. This change takes effect immediately.

Deleting Group Profiles

To delete a group profile:

1. Click the **Groups** option in top menu bar. This opens the **Manage Group Profiles** page.
2. Click the **delete** option next to the desired group.
3. You will be asked to confirm the delete request.

Managing User Profiles

User profiles are created and managed in the same way as group profiles. User profiles always take priority over any group profiles that the user might also be a member of. If you need to ensure that a specific user receives a specific profile configuration, you will want to create a user profile for that user.

Adding, Modifying and Deleting User Profiles

The adding, modifying and deleting of user profiles works just like group profiles. The only difference is there are no priority ordering controls in the user profile list. These are not necessary, as user profiles have a one-to-one relationship with their user.

Invite Users to Install mobilEcho and Enroll in Management

To get started with mobilEcho, users need to install the mobilEcho client application through the Apple App Store. If you are using the mobilEcho Client Management system, they also need to enroll the mobilEcho app on their device with the mobilEcho Client Management system. Once enrolled, their mobilEcho client configuration, security settings, and capabilities are controlled by their mobilEcho user or group profile.

mobilEcho 3.5 includes two device enrollment mode options. This mode is used for all client enrollments. You will need to select the option that fits your requirements:

- **PIN number + Active Directory username and password** - In order to activate their mobilEcho app and gain access to mobilEcho servers, a user is required to enter an expiring, one-time use PIN number and a valid Active Directory username and password. This option ensures that a user can only enroll one device, and only after receiving a PIN number issued by their IT administrator. This option is recommended when the enhanced security of two-factor device enrollment is required.
- **Active Directory username and password only** - A user can activate their mobilEcho app using only their Active Directory username and password. This option allows a user to enroll one or more devices at any point in the future. Users just need to be given the name of their mobilEcho Client Management server, or a URL pointing to their mobilEcho Client Management server, which can be posted on a web site or emailed, simplifying the rollout of mobilEcho to large numbers of users. This option is preferred in environments where two-factor enrollment is not required and many users may need access to mobilEcho at any time, such as student deployments.

To select an enrollment mode:

1. Click the **Devices** option in the top menu bar. This opens the **Manage Devices** page.
2. Select the desired **Device enrollment requires** option.

Inviting a user to enroll

Users are typically invited to enroll in the mobilEcho Client Management system with an email that is sent from the mobilEcho Client Management Administrator. If required by the server, this email contains a one-time use PIN number that is valid for a configurable number of days. The PIN number can be used to enroll the mobilEcho app on one device only. If a user has multiple devices, they will need to be sent one invitation email for each device that needs access. This email includes a link to the mobilEcho app in the Apple App Store, in the case the app first needs to be installed. It also includes a second link that, when tapped while on the device, will open mobilEcho and auto-complete the client enrollment form with the mobilEcho Client Management server's name, the unique enrollment PIN number, and the user's username. By using this link, a user simply enters their account password to complete client enrollment.

Using basic URL enrollment links when PIN numbers are not required:

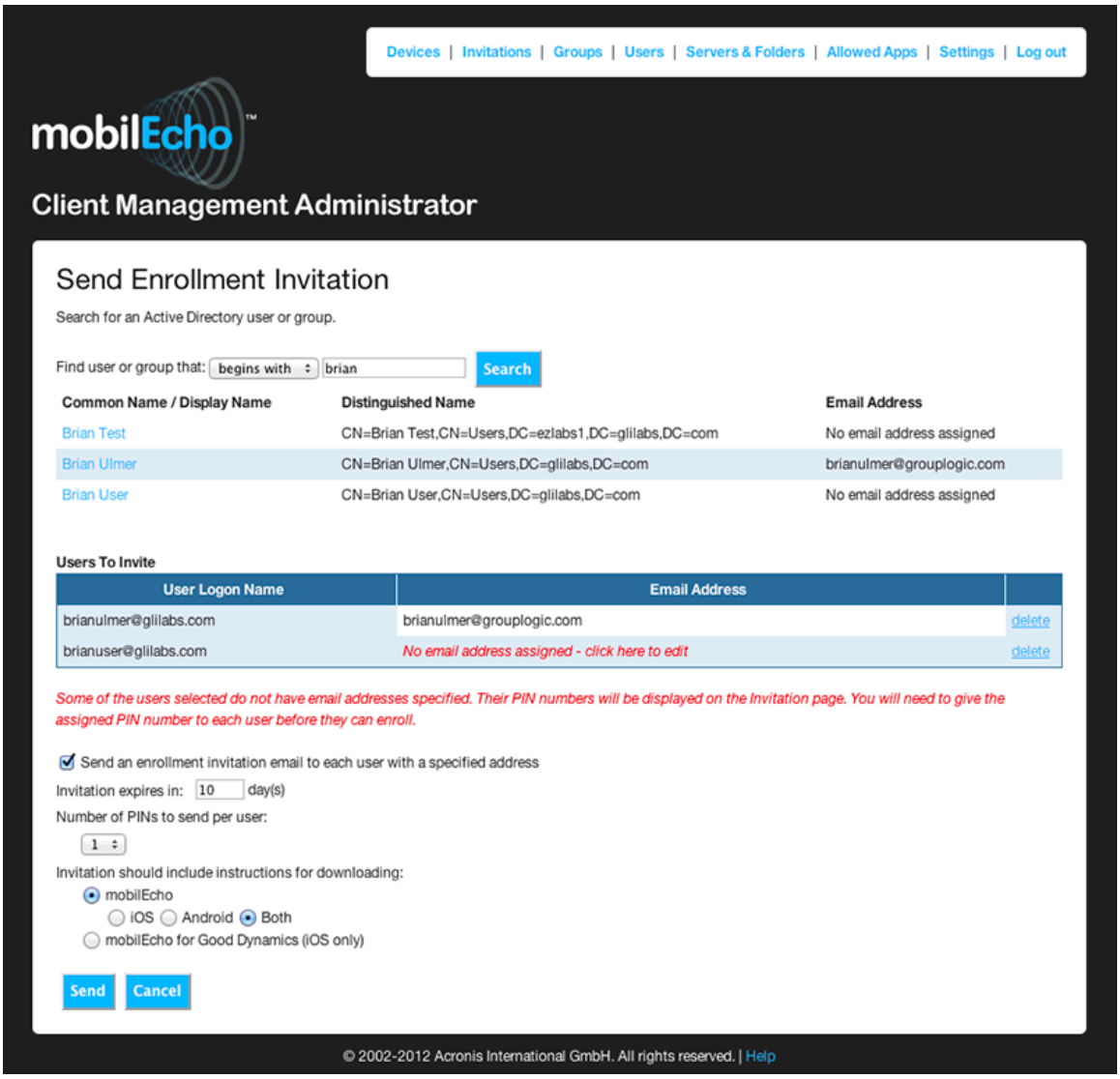
- If your server is configured to not require PIN numbers for client enrollment, you can give your users a standard URL that will automatically start the enrollment process when tapped from the mobile device. To determine the enrollment URL for your management server, click the **Invitations** option in the top menu bar. The URL is displayed on this page.

To generate a mobilEcho enrollment invitation:

1. Click the **Invitations** option in top menu bar. This opens the **Enrollment Invitations** page.
2. Click the **Send enrollment invitation**.
3. Enter an Active Directory user name or group name and click **Search**. If a group is chosen, each email address in that group will be added to the **Users to invite** list. This will allow you to batch invite all members in a group. You can optionally remove one or more of those group members before sending the invitations. You can perform '**begins with**' or '**contains**' searches for Active Directory groups. Begins with search will complete much faster than contains searches.
4. Once you've added your first user or group, you can issue a new search and continue to add additional users or groups to the list.
5. Review the list of **Users to invite**. You can **Delete** any users you would like to remove them from the list.
6. If a user does not have an email address associated with their account, you will see **No email address assigned - click here to edit** in the **Email Address** column. You can click any of these entries to manually enter an alternate email address for that user. If a user is left with **No email address assigned**, a PIN number will still be generated for them, and will be visible on the **Enrollment Invitations** page. You will need to convey this PIN number to the user by another means before they can enroll their mobilEcho client.
7. If you prefer to manually communicate enrollment PIN numbers to their users, you can uncheck the **Send an enrollment invitation email to each user with a specified address** option. Each PIN number will be visible on the **Enrollment Invitations** page.
8. Choose the number of days you'd like the invitation to be valid for in the **Invitation expires in** field.
9. Choose the **number of PINs**you'd like to send to each user on the invitations list. This can be used in cases where a user may 2 or 3 devices. They will receive individual emails containing each unique one-time-use PIN.
    a. *Please Note: mobilEcho licensing allows each licensed user to activate up to 3 devices, each additional device beyond 3 is counted as a new user for licensing purposes.*
10. Choose the version or versions of the mobilEcho client that you would like your users to download and install on their device. You may choose **iOS**, **Android**, or **Both**. If you are using **mobilEcho for Good**

Dynamics, you can select that option and your users will only be directed to download the Good Dynamics version of mobilEcho.

11. Click Send.
12. If you get an error message when sending, confirm that the SMTP settings in your **mobilEcho_manager.cfg** file are correct. The default location of this file is: **C:\Program Files\Group Logic\mobilEcho Server** on **32-bit** versions of Windows and **C:\Program Files (x86)\Group Logic\mobilEcho Server** on **64-bit** versions of Windows. Changes to this file require a restart of the **mobilEcho Management** service (using the Windows services control panel) to take effect.



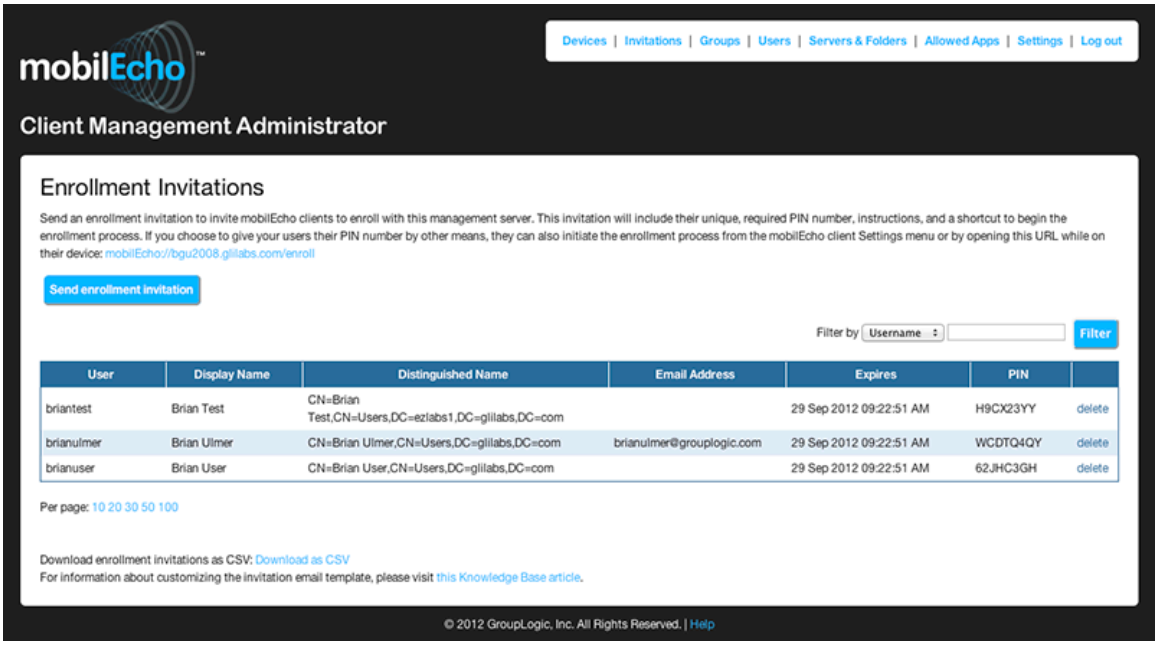
Once an enrollment invitation is generated, the invited users are displayed on the **Enrollment Invitations** page. Each user's PIN number is listed, in the case that you need to communicate it by a means other than the automatic email.

Once a user successfully enrolls their mobilEcho client using their one-time use PIN number, they will no longer appear in this list.

To revoke a user's invitation PIN number, click **delete** to remove them from the list.

Filter by - The invitations list can be filtered by Username, Display Name, or Email Address.

Download enrollment invitations as CSV - The entire or filtered invitations list can be exported to a CSV file and opened in Excel or imported into a custom process.

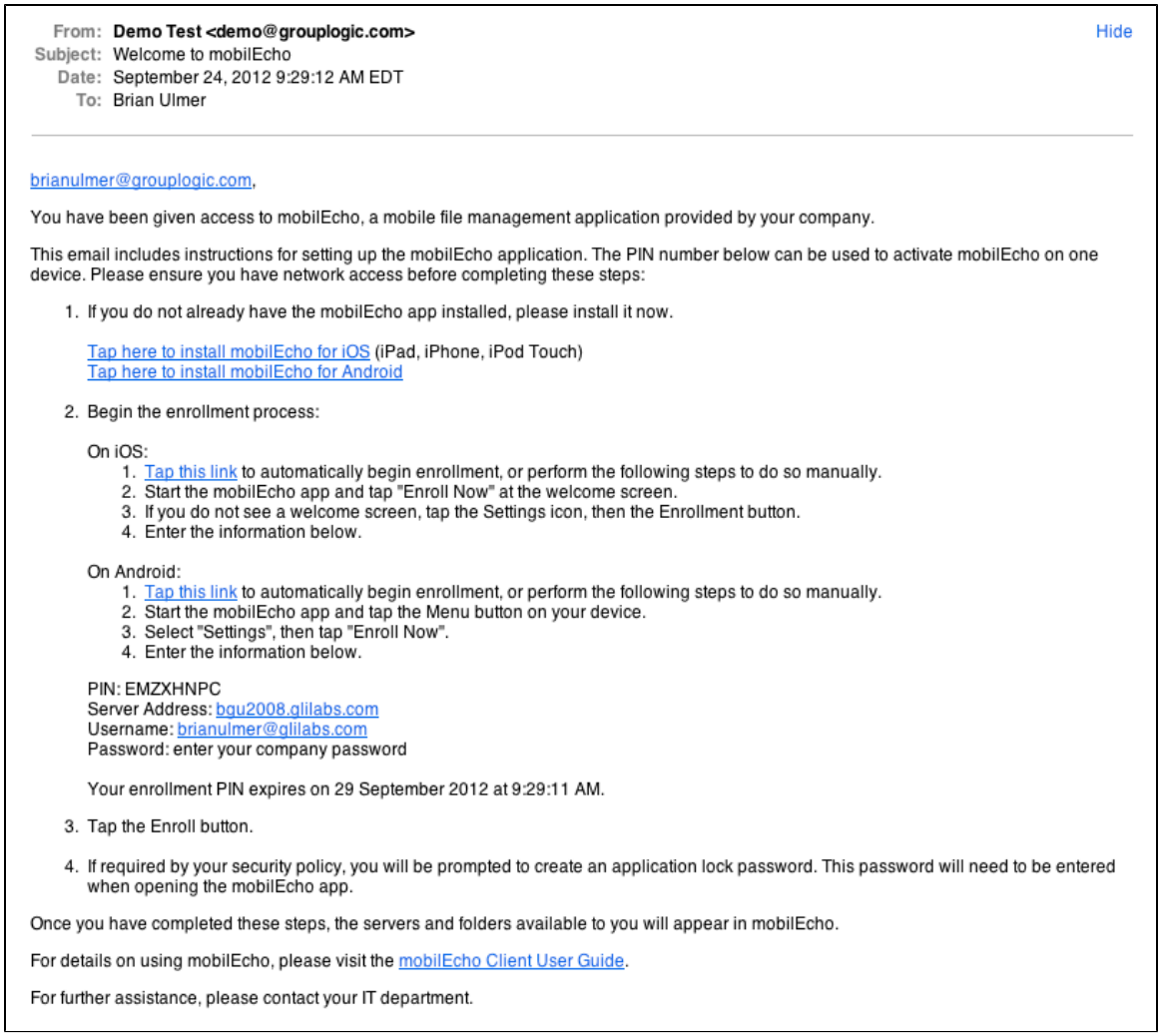


User-side Management Enrollment Process

Each user sent a mobilEcho management enrollment invitation will receive an email that contains:

- A link to install mobilEcho from the Apple App Store
- A link used to launch the mobilEcho app and automate the enrollment process
- A one-time use PIN number
- Their management server address

The email guides them through the process of installing mobilEcho and entering their enrollment information in the mobilEcho client app.



From: **Demo Test <demo@grouplogic.com>** Hide
Subject: Welcome to mobilEcho
Date: September 24, 2012 9:29:12 AM EDT
To: Brian Ulmer

brianulmer@grouplogic.com,

You have been given access to mobilEcho, a mobile file management application provided by your company.

This email includes instructions for setting up the mobilEcho application. The PIN number below can be used to activate mobilEcho on one device. Please ensure you have network access before completing these steps:

1. If you do not already have the mobilEcho app installed, please install it now.

   Tap here to install mobilEcho for iOS (iPad, iPhone, iPod Touch)
   Tap here to install mobilEcho for Android

2. Begin the enrollment process:

   On iOS:
   1. Tap this link to automatically begin enrollment, or perform the following steps to do so manually.
   2. Start the mobilEcho app and tap "Enroll Now" at the welcome screen.
   3. If you do not see a welcome screen, tap the Settings icon, then the Enrollment button.
   4. Enter the information below.

   On Android:
   1. Tap this link to automatically begin enrollment, or perform the following steps to do so manually.
   2. Start the mobilEcho app and tap the Menu button on your device.
   3. Select "Settings", then tap "Enroll Now".
   4. Enter the information below.

   PIN: EMZXHNPC
   Server Address: bgu2008.glilabs.com
   Username: brianulmer@glilabs.com
   Password: enter your company password

   Your enrollment PIN expires on 29 September 2012 at 9:29:11 AM.

3. Tap the Enroll button.

4. If required by your security policy, you will be prompted to create an application lock password. This password will need to be entered when opening the mobilEcho app.

Once you have completed these steps, the servers and folders available to you will appear in mobilEcho.

For details on using mobilEcho, please visit the mobilEcho Client User Guide.

For further assistance, please contact your IT department.

If mobilEcho has been installed, and the user taps the "**Tap this link to automatically begin enrollment...**" option while viewing this email on their device, mobilEcho will automatically launch and the enrollment form will be displayed. The user's server address, PIN number, and username are also encoded in this URL, so these fields are auto-completed in the enrollment form. At this point, the user simply has enters their password to complete the enrollment process.

The username and password required are the user's Active Directory username and password. These credentials are used to match them to the proper user or group management profile, and for access to mobilEcho file servers, if their management profile allows the saving of their credentials for mobilEcho server logins.

If their mobilEcho management profile requires an application lock password, they will be prompted to enter one. All password complexity requirements configured in their profile will be enforced for this initial password, and for any change of their application lock password in the future.

If their profile restricts the local storage of files on their device, they will be warned that existing files will be removed and allowed to cancel the management setup process if there are files they need to deal with before they are removed.

Ongoing Management Updates

After the initial management setup, mobilEcho clients will attempt to contact the management server each

time the client app is started. Any settings changes, server or folder assignment changes, application lock password resets, or remote wipes will be accepted by the client app at that time.

> **Client management connectivity requirements**
>
> mobilEcho clients must have network access to the management server in order configure management and to receive profile updates, remote password resets, and remote wipes. If your client is required to connect to a VPN before they can access mobilEcho file servers, they will also need to VPN before management commands will be accepted.

Managing mobilEcho Devices

Once a mobilEcho client has enrolled in the mobilEcho Client Management System, their mobile device will appear on the **Manage Devices** list. This list gives detailed status information for each device that has been activated with a PIN number, or previously managed by a mobilEcho 2.1 or earlier server, if that option is enabled.

> **Migration of existing, managed mobilEcho 2.X clients to mobilEcho 3.0**
>
> mobilEcho 2.X did not require a PIN number to enroll a client in the mobilEcho Client Management system. There are two options for migrating mobilEcho 2.X clients to the 3.0 management system. By default, mobilEcho servers that are upgraded from 2.X to 3.0 allow clients previously managed by the 2.X server to auto-enroll and appear in the mobilEcho 3.0 devices list without having to enter a PIN number. If you would like to ensure that all devices accessing the system have enrolled with a PIN number, you can disable this setting. In that case, if the user doesn't have "User can remove mobilEcho from management" privileges, the user will need to delete mobilEcho from their device and reinstall a new copy from the App Store before they can enroll using a PIN number.
>
> Also note that when this auto-enroll setting is enabled, it will be possible to do an iTunes backup of a device running a managed version of mobilEcho 2.X or 3.0, restore that backup to a new device, and as long as the user has the active directory username and password for the associated account, that new device can be automatically enrolled in mobilEcho without a PIN number.
>
> It is recommended that you disable the auto-enroll setting after your previously managed clients have all accessed the management server for the first time. They will appear in the **Manage Devices** list when this happens.

To allow mobilEcho clients that were already enrolled in mobilEcho 2.X Client Management to automatically enroll after your mobilEcho Client Management server is upgraded to 3.0, enable the **Allow mobilEcho clients previously managed by 2.X servers and managed mobilEcho clients restored to new devices to auto-enroll without PIN** setting.

To invite user(s) to enroll their devices, click **Send enrollment invitation**. This begins the same process as detailed above in the *Inviting a user to enroll* section.

The device table contains the following information on each managed device:

- **Display Name** - the user's Active Directory (AD) full name

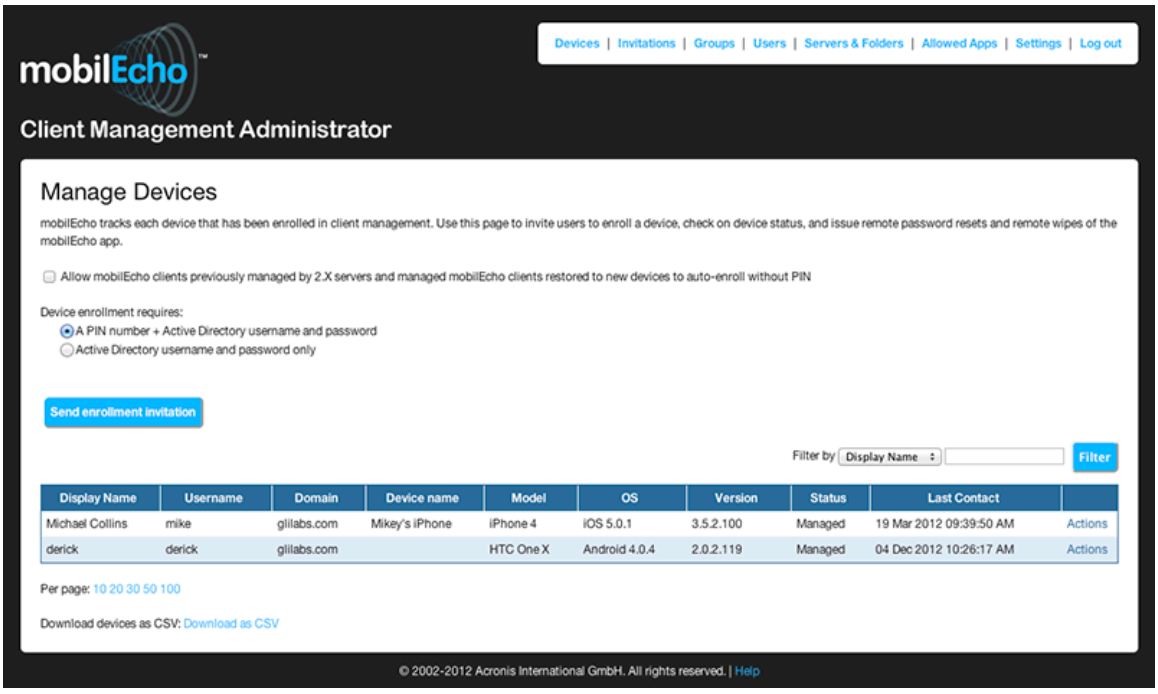
- **Username** - the user's AD account username
- **Domain** - the domain that the user's AD account is a member of
- **Device name** - the device name set by the user
- **Model** - the device model/type
- **OS** - the device's OS version
- **Version** - the mobilEcho app version on the device
- **Status** - the status of the mobilEcho app on the device
- **Last Contact** - the last time this device contacted the mobilEcho management server

The each device includes an **Actions** menu. Device actions include:

- **More info** - show additional details about the device, including device unique ID and editable device Notes field.
- **App password reset** - remotely reset the mobilEcho application lock password on that device.
- **Remote wipe** - remotely wipe all mobilEcho data and settings on that device. No other apps or OS data is effected.
- **Remove from list** - remove the device from mobilEcho management without wiping it. This is typically used to remove a device that you do not expect to ever contact the mobilEcho Client Management server again. If you have enabled "*Allow mobilEcho clients previously managed by 2.X servers and managed mobilEcho clients restored to new devices to auto-enroll without PIN*", a device removed from the list will automatically reappear and become managed again if it ever makes contact with the server in the future.

Filter by - The devices list can be filtered by Username or Display Name.

Download devices as CSV - The entire or filtered devices list can be exported to a CSV file and opened in Excel or imported into a custom process.



Performing Remote Application Password Resets

The mobilEcho client can be secured with an Application Lock Password that must be entered when mobilEcho is launched. If a user forgets this password, they will not be able to access mobilEcho. The

mobilEcho app password is independent of the user's Active Directory account password.

When a password is lost, the only recourse a user has is to uninstall mobilEcho from their device and reinstall it. This deletes any existing data and settings, which maintains security but will likely leave them with no access to mobilEcho servers until they are sent a new management invitation.

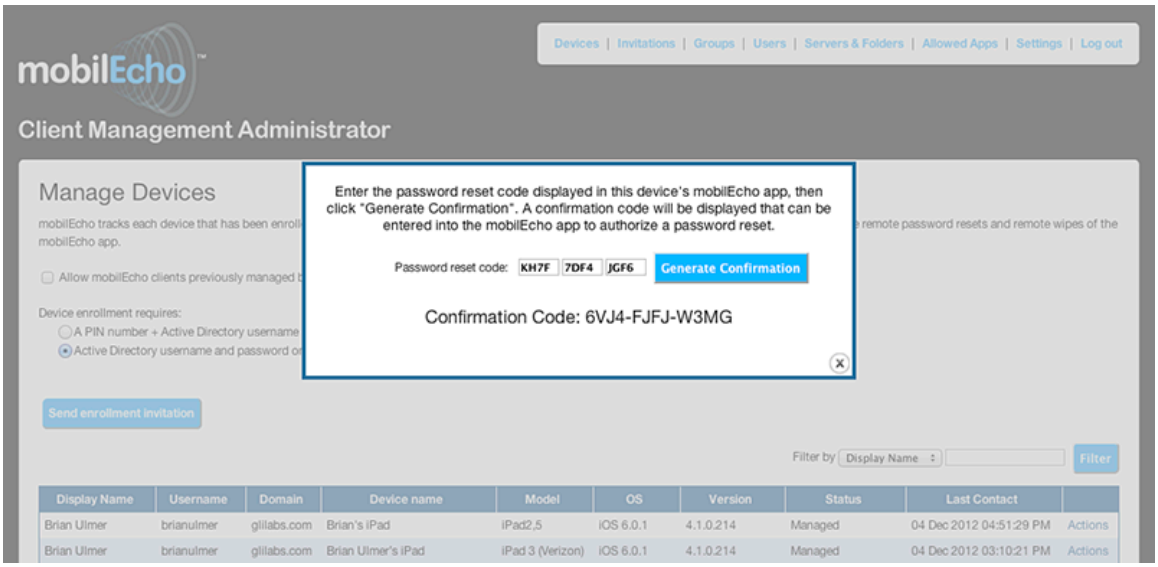
To avoid these issues, the mobilEcho Client Management system can perform a remote application password reset.

Reset an Application Password - mobilEcho for iOS version 4.1 or later

mobilEcho on-device files have always been protected using Apple Data Protection (ADP) file encryption. To further protect files on devices being backed up into iTunes and iCloud, devices without device-level lock codes enabled, and as a general security enhancement, mobilEcho 4.1 introduced a second layer of full-time custom encryption applied directly by the mobilEcho app. One aspect of this encryption is that mobilEcho 4.1 and later can no longer have their application lock password reset over the air. Instead, a password reset code and confirmation code must be exchanged between the device user and the mobilEcho IT administrator, in order to enable mobilEcho to decrypt it's settings database and allow the user to set a new app password.

To reset a mobilEcho for iOS 4.1 or later application password:

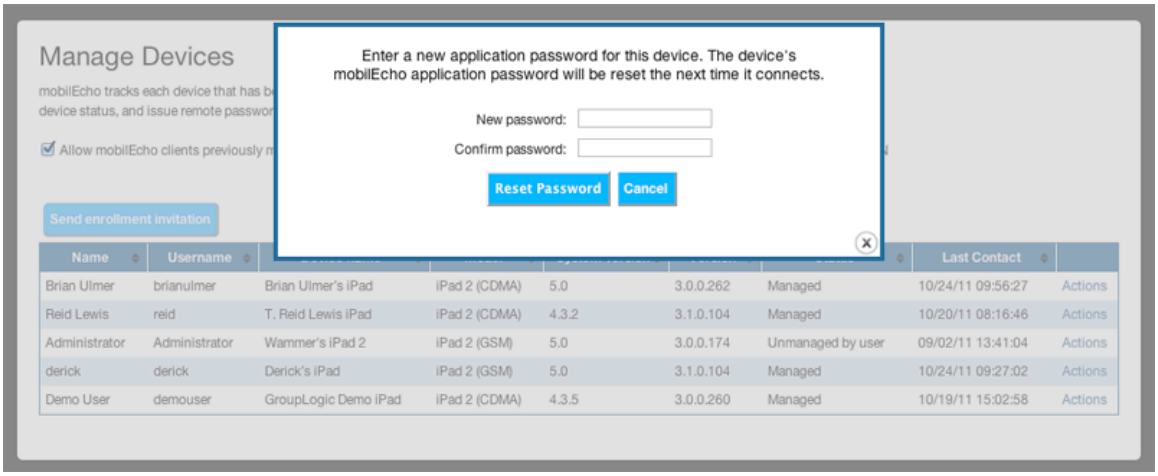
- An end user will contact you requesting to have their mobilEcho app password reset, they will give you their **Password Reset Code**
- Click the **Devices** option in the top menu bar.
- On the **Manage Devices** page, find the device you'd like to issue an app password reset for and click the **Actions** menu link.
- Click **App password reset...**
- Enter the **Password Reset Code** given to you by the user, then click **Generate Confirmation**
- Tell or email the user the **Confirmation Code** that is displayed
- The user will enter this code into the app's password reset dialog and will then be prompted to set a new password. If they abort this process without setting a proper app password, they will continue to be denied access to mobilEcho an will have to repeat the app password reset process.



Reset an Application Password - mobilEcho for iOS version 4.0.2 or earlier

To reset a mobilEcho for iOS 4.0.2 or earlier application password:

- Click the **Devices** option in the top menu bar.
- On the **Manage Devices** page, find the device you'd like to issue an app password reset for and click the **Actions** menu link.
- Click **App password reset...**
- Enter and confirm the new password and click **Reset Password**.
- A 'Pending app password reset' status will appear in the **Status** column for that device. When the password reset has been accepted by the device, its **Status** will return just saying 'Managed'.
- App password resets can be canceled at any time before the client next connects to the management server. This option appears in the **Actions** menu after a password reset has been issued.



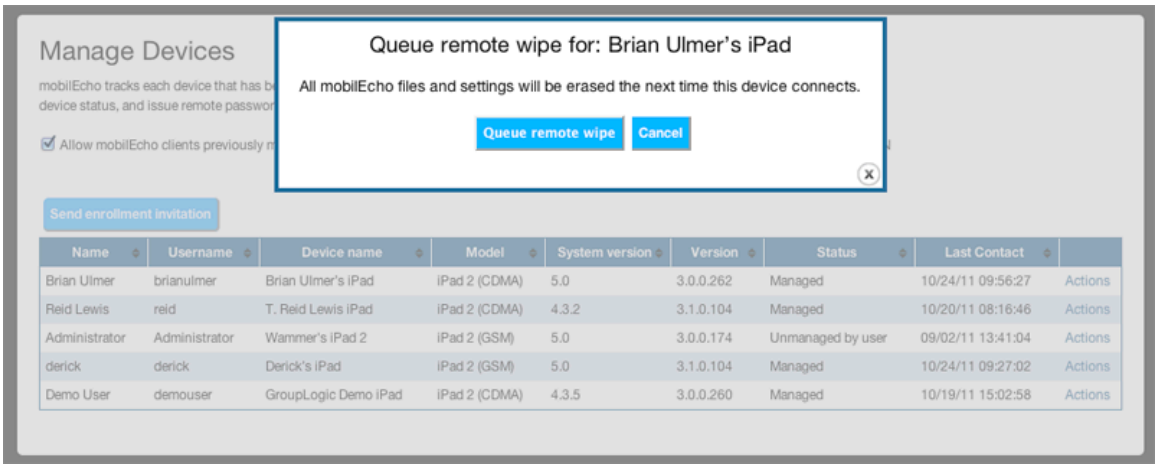
Performing Remote Wipes

mobilEcho Client Management allows a mobilEcho client application to be remotely wiped. This selective remote wipe removes all files that are locally stored or cached within the mobilEcho app. All mobilEcho settings are reset to previous default settings and any servers that have been configured in the app are removed.

Queueing a Remote Wipe

To issue a remote wipe:

- Click the **Devices** option in the top menu bar.
- On the **Manage Devices** page, find the device you'd like to issue a remote wipe for and click the **Action s** menu link.
- Click **Remote wipe...**
- Confirm the remote wipe by clicking **Queue remote wipe**.
- A 'Pending remote' status will appear in the **Status** column for that device. When the remote wipe has been accepted by the device, its **Status** will reflect this.
- Remote wipes can be canceled at any time before the client next connects to the management server. This option appears in the **Actions** menu after a remote wipe has been issued.



Client management connectivity requirements

mobilEcho clients must have network access to the management server in order to receive remote wipes. If your client is required to connect to a VPN before they can access mobilEcho file servers, they will need VPN access before remote wipes will be accepted.

mobilEcho Server Backup and Restoration

mobilEcho Server Architecture Overview

mobilEcho's server-side software consists of two services that together provide the full suite of mobilEcho server-side functionality. mobilEcho servers can have two simultaneous roles: **File Access Server** and **Cl ient Management Server**. The **File Access Server** role is enabled on all mobilEcho servers and is required for mobilEcho to function. The **Client Management Server** role is optional and often only enabled on a single mobilEcho server.

These two roles run as separate services that can be found in the Windows **Services** control panel:

- **mobilEcho File Access Server for Mobile Devices** – This service is enabled on every mobilEcho server. It handles all communication with mobile clients, including client authentication, file browsing, and file transfers. If a mobilEcho server is configured to perform mobilEcho Client Management, this service also communicates client management settings, remote password reset commands, and remote wipe commands to the mobilEcho client app.
- **mobilEcho Management** – This service is initially disabled when you install mobilEcho for the first time. If you wish to use a specific mobilEcho server as a mobilEcho Client Management Server, you can configure and enable this service. Full details on this process are included in the mobilEcho Client Management Server User Manual. Once enabled, this service provides a web-based interface for creating mobilEcho client management profiles and enrolling users in the mobilEcho client management system.

These two services store their configuration and settings in separate locations on a Windows server. This document details the process for backing up and restoring all the configuration, settings, and client management information that is needed to recover or migrate a mobilEcho server. mobilEcho has the ability to provide access to files stored directly on the server it is running on. Steps to back up these files are not included in this document. Please ensure that these files are included in your server backup routine if necessary.

Backing up a mobilEcho File Access Server's volumes and configuration

Registry Backup

All of the **mobilEcho File Access Server's** volume and configuration settings are stored in the Windows registry. To back up these settings, find the Paramaters4 folder in the registry at this location and Export it. This will generate a '**.reg**' file containing the required registry settings.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mobilEcho\Parameters4

Restoring a mobilEcho File Access Server's volumes and configuration

Install mobilEcho on a new server

Perform a default mobilEcho server installation on the new Windows server. Then, start the **mobilEcho Administrator** application, click the **Licensing** button, and enter your serial number.

Locally-stored shared files

If your mobilEcho server was configured with volumes that share files located locally on the mobilEcho server, you will need to restore or move these files to the new server before mobilEcho can share these volumes.

mobilEcho's **Volumes** settings in the registry refer to local volume locations by drive letter. If the drive letters of your local storage have changed in moving to a new server, these drive letters will need to be corrected before the volumes located on that storage can be shared. This can be done by editing the **Volumes** keys in the registry directly, or by removing and recreating the affected volumes using the **mobilEcho Administrator** application.

mobilEcho network reshare volumes are configured using the UNC path to the remove storage location, rather than drive letter, so they will work immediately once the backed up registry settings are restored.

Registry Restoration

Copy the '**.reg**' file, that you previously exported, to any location on the new Windows server and double-click it. You will be asked to confirm that you want to import the settings. Click **Yes**.

Service Restart

Open the Windows **Services** control panel, select the **mobilEcho File Access Server for Mobile Devices** service, and **Restart** the service.

Backing up a mobilEcho Client Management Server's configuration, profiles, and database

Configuration File

Back up the '**mobilEcho_manager.cfg**' file. It contains your mobilEcho Client Management Server configuration settings. This file is located here:

C:\Program Files (x86)\Group Logic\mobilEcho Server\ManagementUI\mobilEcho_manager.cfg

User and Group Profiles

Back up the entire '**Management**' directory. It contains the User and Group Profiles configured on your management server and the defined priority order of the Group Profiles. This directory is located here:

C:\Program Files\Group Logic (x86)\mobilEcho Server\Management\

Database

Back up the mobilEcho Client Management Server database files. These database files contain the records of all client devices enrolled in the client management server, the assigned servers and folders you've added to the client management server, the enrollment invitations and PIN numbers that gave been generated, and many other important items. Back up these 3 specific files only:

- development.sqlite3
- production.sqlite3
- schema.rb

These files are located here:

C:\Program Files\Group Logic (x86)\mobilEcho Server\ManagementUI\db\

Restoring a mobilEcho Client Management Server's configuration, profiles, and database

Install mobilEcho on the new server

If not already done in the process of restoring your mobilEcho File Server settings, perform a default mobilEcho server installation on the new Windows server. If you've already installed mobilEcho Server, you can skip this step.

Configuration File

Restore the '**mobilEcho_manager.cfg**' file to the new server. You can simply overwrite the default version created during installation, or you can first rename it if you'd like to keep it for reference.

> **Important Setting Verification**
>
> You will need to ensure that the DNS name specified in this file for the **MANAGEMENT_SERVER_ADDRESS** setting is configured in your DNS to point to the new server's IP address. If this is not done, existing managed mobilEcho clients, that are configured to use this DNS name, will attempt to contact this DNS name and not be able to reach the new version of the client management server.

This file is restored to this location:

C:\Program Files (x86)\Group Logic\mobilEcho Server\ManagementUI\mobilEcho_manager.cfg

User and Group Profiles

Replace the contents of the '**Management**' directory with the full contents of the backed up version. This directory is located here:

C:\Program Files\Group Logic (x86)\mobilEcho Server\Management\

Database

Replace the existing 3 database files in the '**db**' directory with the database files that were backed up. These 3 files are:

- development.sqlite3
- production.sqlite3
- schema.rb

These files are restored to this folder:

C:\Program Files\Group Logic (x86)\mobilEcho Server\ManagementUI\db\

> **Mandatory database schema update**
>
> Once these 3 files have been copied to the '**db**' directory, you must run the **setup_db.bat** fil e to update the database schema. This file is also located in the '**db**' directory. **This has to be done before starting the mobilEcho Management service.**

Start the mobilEcho Management service

Open the Windows **Services** control panel, open the **Properties** for the **mobilEcho Management** servic e, set the **Startup Type** to **Automatic**, and **Start** the service. You should now be able to log into the mobilEcho Client Management Administrator web interface at: https://servername.companyname.com:30 00 (or whichever alternate port you may have configured the web interface to run on within the '**mobilEch o_manager.cfg**' file).

Verify all preexisting devices, profiles, and settings are displayed in the web interface.

mobilEcho enrollment invitations

Configuring custom invitations

You can configure your own invitation emails. To do so, navigate to **C:\Program Files (x86)\Group Logic\mobilEcho Server\ManagementUI\config\locales\views\mailers** and choose one of these files:

- de.yml - This is the file for German invitations.
- en.yml - This is the file for English invitations.
- fr.yml - This is the file for French invitations.
- ja.yml - This is the file for Japanese invitations.

You can create your own, custom invitations, by editing these files to suit your preferences. You should edit only the text in brackets (**"this"**) as the rest are keywords for the mobilEcho server. Click on the links to download the defaults.

> When upgrading mobilEcho server, the custom invitations will not be upgraded. They will continue to use your custom text but the Subject will be localized.

Localization

In mobilEcho 4.2 there is a new config file dealing with the localization of the Subject text in mobilEcho invitation emails.

The file is located in **C:\Program Files (x86)\Group Logic\mobilEcho Server\ManagementUI\mobilEcho_manager_intl.cfg**

If you would like to customize the enrollment email Subject text for French, German, or Japanese, these setting are in the mobilEcho_manager_intl.cfg file. If you have a mobilEcho client in French, German, Japanese or English, you need to have the Windows language pack for the required languages installed on your server in order for the client to receive some of the possible error messages in their native language.

mobilEcho_manager.intl.cfg

```
# Email subject of the invitation (German)
SMTP_EMAIL_SUBJECT_GERMAN = Willkommen bei mobilEcho
# Email subject of the invitation (French)
SMTP_EMAIL_SUBJECT_FRENCH = Bienvenue sur mobilEcho
# Email subject of the invitation (Japanese)
SMTP_EMAIL_SUBJECT_JAPANESE = mobilEcho
```

Note:

The file should be saved using the UTF-8 encoding.

Using certificates with mobilEcho

Before you begin

The file **cacert.pem,** by default, contains a bundle of certificate authority root certificates which the **mobil Echo Server** uses. The **mobilEcho Management Server** generates a self-signed certificate which it uses. This certificate ensures the security and encryption of the connection, but may cause some errors with your browser.

Using other certificates

Instead of using the certificate which mobilEcho generates, you can add your own certificates (self-signed) or get one from a certificate authority.

For the mobilEcho Server

1. Get a certificate from a **Certificate Authority** or generate your own (**self-signed**).
2. After you acquire the certificate, you need to place its contents inside the **cacert.pem** file as follows:
    a. Open your certificate file.
    b. Copy its contents.
    c. Open the **cacert.pem** file (by default in \Program Files (x86)\Group Logic\mobilEcho Server\).
    d. Scroll to the bottom of the file and paste the contents of your certificate.

Note:

Some files contain both the certificate and the public key, while others contain only the certificate or the key. You will need the file which contains both (e.g. .cer contains only a certificate while .pfx contains a certificate and its key in the same file).

For the mobilEcho Managment Server

In this case you need a separate certificate and key or you can convert your bundled one. If the certificate you downloaded is bundled with the key (both are in the same file) you will have to convert the file into two separate files.

1. You will need to edit the **mobilEcho_manager** config file. It is located in the **ManagementUI** folder.
2. Configure the settings for the paths to your **certificate** and **key**. The first one is the path to the key and the second one is the path to the certificate.

mobilEcho_manager

```
# You must restart the service for changes to be applied.
HTTPS_USE_AUTOGENERATED_CERTS = true
HTTPS_KEY = C:\Keys\YourKey.key
HTTPS_CERT = C:\Certificates\YourCertificate.cert
```

3. Set **HTTPS_USE_AUTOGENERATED_CERTS** to **false**. Otherwise, **mobilEcho** will continue using the certificate it generated for itself instead of the one you just set-up.

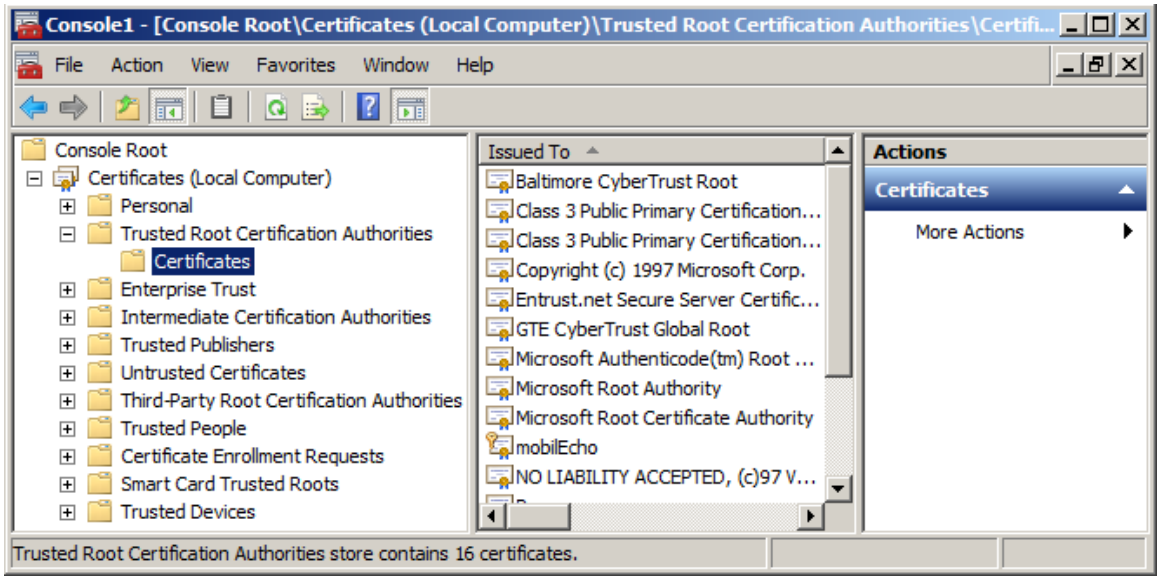
The path shown above to the **.cert** and **.key** files is just an example.

For any added **certificate** you must also configure Windows Server so that it recognizes your certificate as trusted.

Note:

This process will make this certificate trusted by Windows Server and it presents a security risk if you get your certificates from an unauthorized Certificate Authority.

1. To do so, open the **Start menu**.
2. Open **Run**, and type in **mmc**.
3. From the **Console** open the **File** tab.
4. Select **Add/Remove Snap-in...**
5. From the list on the left select **Certificates** and press **Add>**.
6. Select **Computer account** and press **Next**.
7. Select **Local computer** and press **Finish**.
8. Press **OK** to close the dialog and return to the console.
9. Expand the **Certificates** drop-down.
10. Expand the **Trusted Root Certificate Authorities** and click on **Certificates**.



11. Click on the **Action** tab, select **All Tasks**, select **Import...**
12. Through the **Certificate Wizard** browse and select your self-signed certificate as follows:
    a. Press **Next** on the **Certification wizard welcome screen**.
    b. Browse to and select the file you want to import.
    c. Mark **Place all certificates in the following store** and select the **Trusted Root Certification Authorities** store.
    d. Verify that your certificate is in the **Trusted Root Certification Authorities** list.

mobilEcho Client Application User Guide

Welcome to the mobilEcho Client Application User Guide. This document will help you install, configure, and use the mobilEcho iPad application.

> **Send us feedback**
>
> GroupLogic would love to hear your ideas for mobilEcho or about any problems you might encounter. Please email us any time at feedback@grouplogic.com.

Introduction

About mobilEcho

mobilEcho provides iPad and iPhone access to files located on Windows file servers, as well as 'network reshare' access to SMB/CIFS compatible Mac servers, Linux servers and NAS devices. mobilEcho includes two required software components: the mobilEcho File Server and the mobilEcho client application. The server component must be installed on a Windows server before mobilEcho clients can connect. mobilEcho servers can optionally control the mobilEcho client application's features and security settings by configuring the mobilEcho Client Management Server service. The mobilEcho client application can access files on one or many mobilEcho servers. mobilEcho encrypts all network communication using the HTTPS protocol for secure over-the-wire file transfer and stores data on the iPad using Apple Data Protection (ADP) hardware encryption.

mobilEcho Client Application

The mobilEcho client application allows mobile device users to connect to mobilEcho servers to browse and preview server-based files. Files can be copied or synced from servers to on-device encrypted storage within mobilEcho. These files can then be accessed even if the mobilEcho client does not have a Wi-Fi or 3G network connection.

With the mobilEcho client application, files can be opened in other mobile applications, moved, copied, printed, emailed, previewed, renamed or deleted. In addition, the mobilEcho iPad client application allows PDFs to be annotated directly in the mobilEcho application. The mobilEcho client application can accept a management profile from a mobilEcho client management server, allowing IT to configure application settings, capabilities, and security controls. Depending on this client management profile, some of the mentioned mobilEcho application features may be disabled.

mobilEcho Server Software

The mobilEcho server software must be installed on a Windows machine and supports file services as well as management control over the mobilEcho client application. When implementing a client management profile, the IT administrator configures specific settings that manage the mobilEcho client application. These profiles can be created for Active Directory users or groups. For more information about the mobilEcho server, see the mobilEcho Server User Manual.

mobilEcho System Requirements

The mobilEcho server trial version software can be downloaded from:

- http://www.grouplogic.com/enterprise-file-sharing/ipad-file-system/free-trial.html

mobilEcho Client Application Supported devices:

- Apple iPad 1st, 2nd, 3rd, 4th generation
- Apple iPad Mini
- Apple iPhone 3GS, 4, 4S, 5
- Apple iPod Touch
- Android Smartphones and Tablets

mobilEcho Client Application Supported OS's:

- iOS 4.3 or later
- Android 2.2 or later

The mobilEcho Client Application can be downloaded from:

- http://www.grouplogic.com/web/meappstore

Getting Help

GroupLogic offers several sources of help:

- This mobilEcho Client Application User Guide can be reached from the mobilEcho client application **Sett ings** menu.
  - Press the **Settings** button in the application.
  - Press the **Help & Feedback** button.
- For more details on the required mobilEcho server component visit the mobilEcho Quick Start Guide a nd mobilEcho Server User Manual.
- For more information and knowledge base visit the Group Logic support web page at support.grouplogi c.com.

Installing the mobilEcho Client

Installing mobilEcho on your iPad

The mobilEcho client application can be installed for free from the app store of your choosing:

- Click here to open mobilEcho's Apple App Store page
- Click here to open mobilEcho's Android Google Play store page

After the application is installed, tap the mobilEcho icon to open the application. In order to start using the mobilEcho you will need a mobilEcho server to connect to. Visit GroupLogic's web site to download a trial version of mobilEcho Server.

To get familiar with the client application user interface see the mobilEcho Application User Interface secti on of this guide.

For information on configuring your mobilEcho client app, please see Configuring the mobilEcho Client.

INFO

The mobilEcho client application is compatible with iPad 1, 2, 3, or 4, iPhone 3G, 3GS, 4, 4S or 5, and iPod Touch running iOS 4.2 or later.

Go to top

Configuring the mobilEcho Client

Configuring MobilEcho Client Application

Before you start using MobilEcho you will need to:

Configure your application settings - Application Settings Overview

Configure your first server - Server Configuration

Optionally, enroll your mobilEcho client in your company's mobilEcho management system if required - Configuring mobilEcho Client Management

Application Settings Overview

- Application Settings Overview
  - mobilEcho Settings
  - **About mobilEcho**
  - Partner Features
  - Enrollment
  - Management Server
- Setting An Application Password

Application Settings Overview

The mobilEcho client application includes a **Settings** menu where the application's settings can be viewed and modified. Tap on the **Settings** icon

Unknown macro: 'html'

to enter the configuration menu.

When the mobilEcho application has enrolled in mobilEcho client management, a **mobilEcho Management** section will automatically appear in the **Settings** menu, giving information about the server managing the device.

You can exit the **Settings** menu at any time by tapping the **Home** or **Done** buttons.

The following options are available in the **Settings** menu:

mobilEcho Settings

Default Action – Defines what happens when you tap on a file. The available options are: **Nothing**, **Prev iew**, and **Action Menu**.

Local Cache – Controls the amount of device storage space the mobilEcho application can use to temporarily cache files so that they don't have to be re-downloaded from the server when they are reopened. ***This setting does not limit the total size of files you can sync to the device or you can copy into the My Files local folder.*** You can clear the cache by tapping the **Clear Cache** button, located inside the **Local Cache** menu.

Timeout -- Sets the amount of time the mobilEcho client will wait for a server to respond before giving up.

Confirm Deletes – If set to **ON**, you will be asked to confirm each time you delete a file or folder.

App Password – Enables and sets an application password. This password will be required when opening the mobilEcho application. *If you have Good Dynamics integration enabled, the application password is controlled by Good Dynamics and you will not see this item in the settings list.*

- **App Password** – When set to **ON**, an app password will be required when starting the mobilEcho application. If the application password is currently enabled, you will be prompted to enter the current password in order to turn off the setting.
- **Require** – Sets how often the app password is required. The default of **Every Time** will require you

enter your app password any time you leave mobilEcho and return. You can instead set **Require** to a grace period. If you leave mobilEcho and return before the grace period elapses, you will not have to enter your app password.

- **Change Password** – This option appears after an application password is set and can be used to change the existing password. When changing your password, you will first be asked to enter your existing app password.

> **WARNING:**
>
> Note that if you set a password and forget it, you will need to remove the mobilEcho application and reinstall it from the App Store. This will delete all files stored in mobilEcho and reset all your settings.
>
> If your mobilEcho client is enrolled in mobilEcho client management, your IT administrator may be able to reset your App Password remotely.

Certificate -- User identity certificates can be added to the mobilEcho client app. If you are using an HTTPS Reverse Proxy server to access to your mobilEcho server(s), the installed certificate can be used to authenticate with the proxy server. This **Certificate** setting shows the status of the installed certificate. mobilEcho accepts .PFX and .P12 certificate files. More details can be found in the GroupLogic Knowledge Base .

> **NOTE:**
>
> If the mobilEcho application is managed by your corporate mobilEcho Client Management system, some of the **mobilEcho Settings** may be locked by your system administrator.

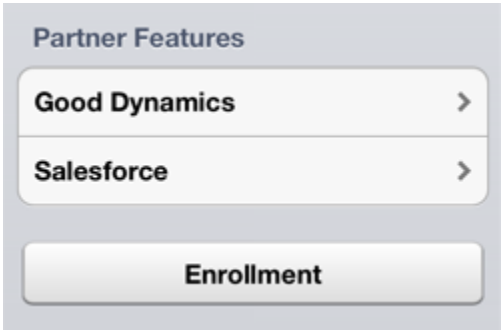
About mobilEcho

Version – Displays the version of the mobilEcho application installed on your device.

Cached Files – Shows the total size of the cached files mobilEcho has created on your device.

Acknowledgements – Contains license details on software components used by mobilEcho.

Partner Features



Good Dynamics - To enroll the mobilEcho app in Good Dynamics, tap this item. This will begin the Good Dynamics enrollment process. You will need an Access Key sent to you by your IT administrator which will have to be entered, along with your email address, to complete Good Dynamics enrollment. For more details on Good Dynamics, please see the mobilEcho for Good Dynamics manual page.

Salesforce - mobilEcho Salesforce integration is configured completely from the server side. This feature allows certain files

to be configured to require that an activity is logged in
Salesforce before they can be opened. Tap this item to view a list of the folders within your mobilEcho app that require Salesforce activity logging.

Enrollment

Enrollment -- If required by your IT department, tap this button to begin the mobilEcho Client Management enrollment process. This process will require a Server Name and PIN number that your IT administrator will send you. You will typically receive an email that includes this information. It will include instructions and should contain a link in step 2 of the process. Open this email on your device and tap the link in step 2 to automatically start the mobilEcho enrollment process. By using this link to begin the process, your Server Name, PIN number, and username will be completed automatically. Simply enter your company account password and tap **Enroll Now** to continue.

Management Server

If your mobilEcho client application is managed by your corporate mobilEcho Client Management system, you may also see these settings:

Use Management – If permitted by your management profile, this option allows you to remove the management profile from your device. If you choose to remove your device from management, you may be prompted that this action will erase your mobilEcho data and settings. You will have the option to cancel at that point, before anything is erased.

Server – Displays the address of the server that manages your mobilEcho client application.

> **NOTE:**
>
> Note that this section is available only if the mobilEcho user has accepted a management policy from a server. If the mobilEcho client application is not managed this section will not appear.

Setting An Application Password

An application password can be set manually from the mobilEcho **Settings** menu or automatically when accepting a management policy. If the management policy does not require an application password, you can set one manually.

To set a mobilEcho App Password:

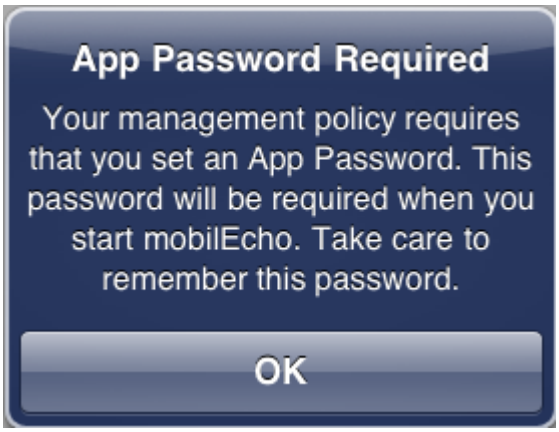
1. Tap the **Settings** icon.
2. Tap the **App Password** option.
3. Turn **ON** the App Password.
4. Enter an application password and confirm it, then tap **OK**.

5. Set the **Require** option. This setting determines how long you can leave mobilEcho and not have to enter your password upon returning.

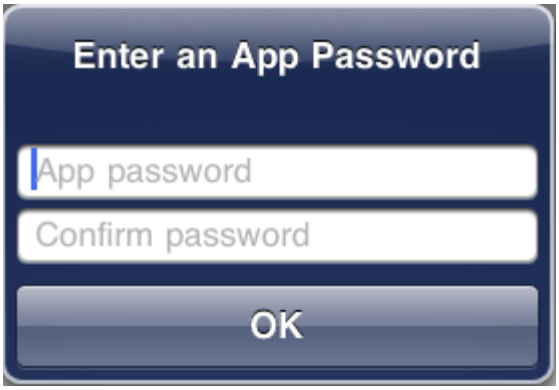
To change your current application password tap **Change Password**, which is available after a mobilEcho app password has been configured. If you change your application password, you will be prompted to enter your current password before you enter the new one.

If your client management profile requires an application password to be set, follow these steps:

1. After initiating mobilEcho Client Management setup, mobilEcho will prompt you to create a password.



2. Enter and confirm a password, then tap **OK**.



3. If your password does not meet the profile's complexity requirements, you will be prompted to enter a new password.

4. To later change your current application password, tap the **Change Password** option. If you change your application password, you will be prompted to enter your current password before you enter the new one.

The mobilEcho system administrator may require a password to be set by the application user and entered any time the mobilEcho application is started. If your mobilEcho client app is managed and an application password is required by your system administrator, the **App Password** setting cannot be disabled from the mobilEcho application.

Server Configuration

- Viewing Servers in the Home navigation pane
- Adding a New Server
- Connecting to a Server
- Editing Your Servers
- Deleting an Existing Server

Viewing Servers in the Home navigation pane

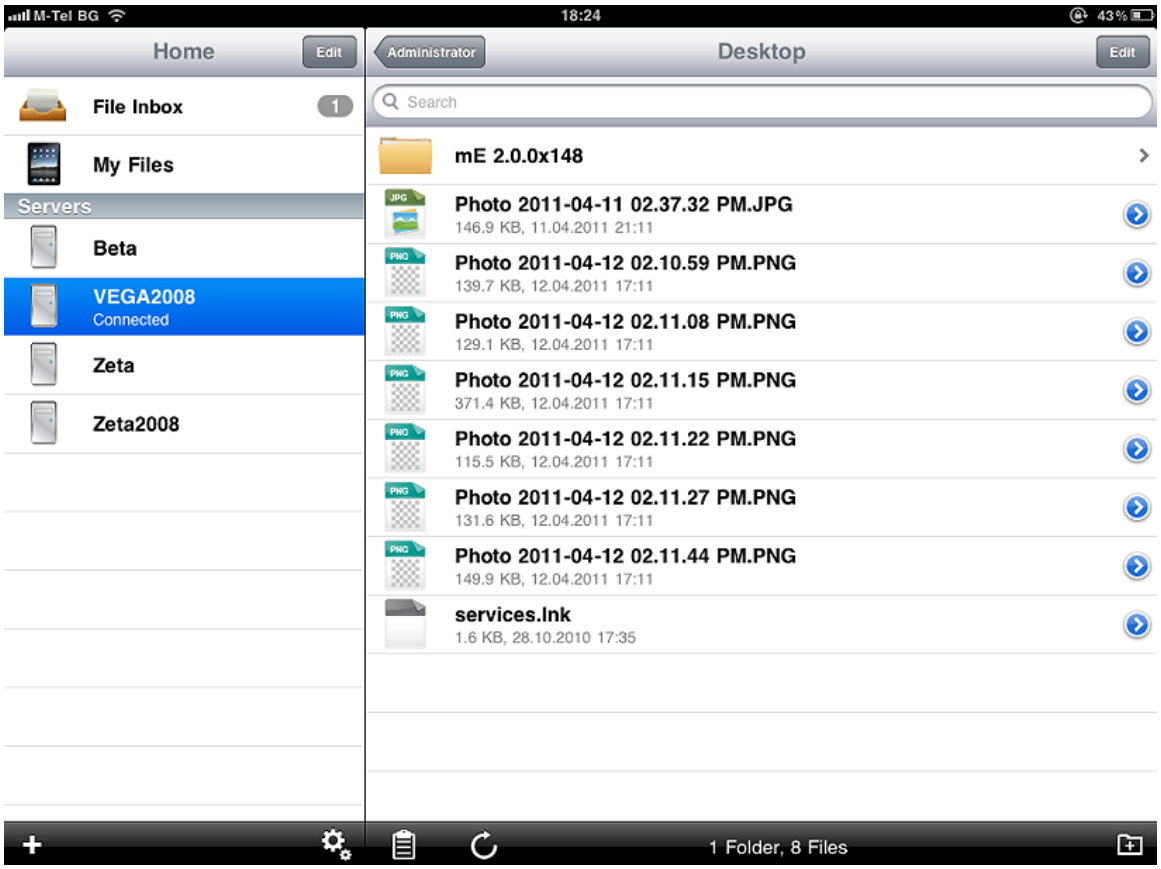
The servers that have been configured in the mobilEcho application are listed in the **Servers** section of the **Home** navigation pane.

Simply tap a server to connect to it. A server's connection state is displayed next to the server name. For more information see Connecting to a Server.

> If your mobilEcho client is managed by a mobilEcho management server, servers may be automatically added to the mobilEcho **Home** screen. Your management profile may also disable your ability to add new servers.

The **Home** pane contains two buttons used to manage servers.

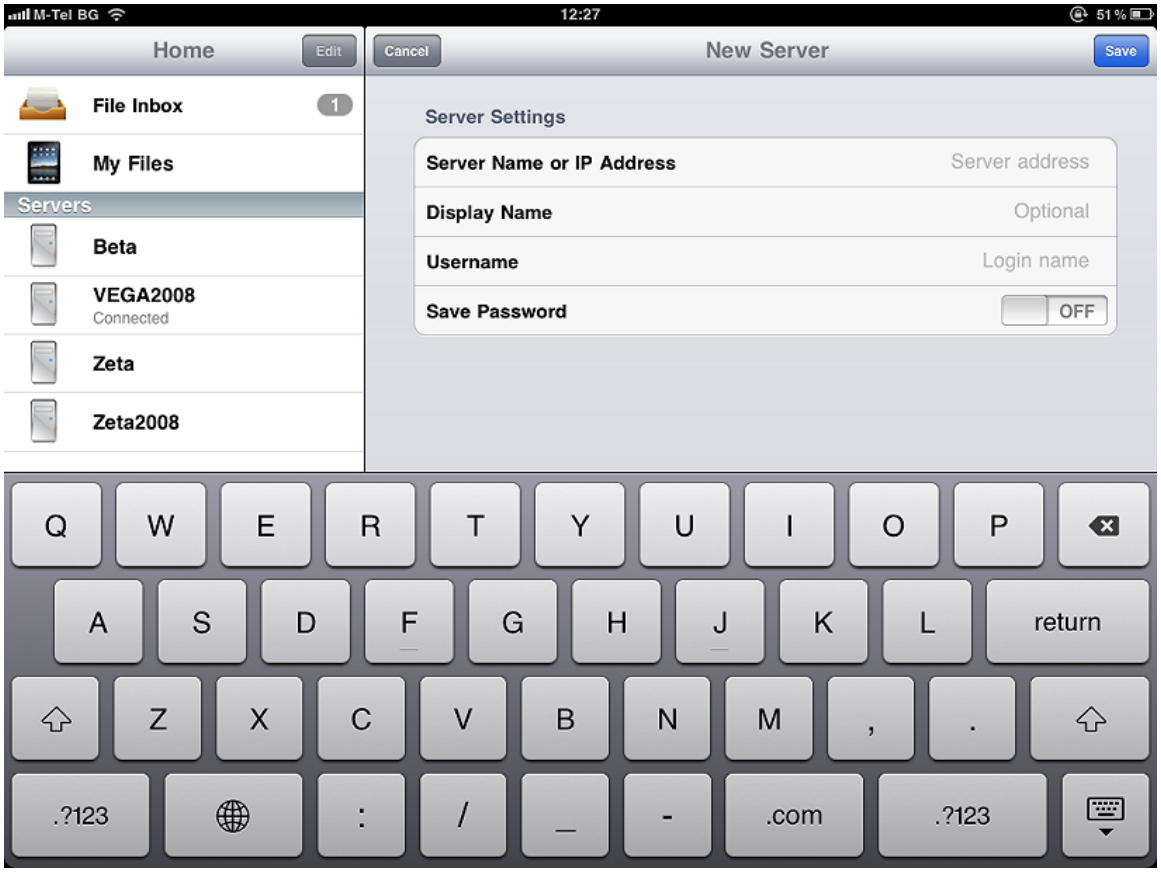
1. **Edit** button – used to modify existing server settings. For more information see Editing Your Servers.
2. Add Server button [+] – used to add a new server to the **Servers** list. For more information see Adding a New Server.



Adding a New Server

Servers must be added to the mobilEcho client application before you can connect to them. It is possible that you already have servers listed that were configured automatically by your mobilEcho management server.

> Depending on the IT policy settings, the mobilEcho client application user may be limited to only connect to specific preassigned servers.



To add a server:

1. Tap the **Add Server** "**+**" button.
2. Select the **Server Name or IP Address** field and enter the Server address. You can enter the server DNS name or IP address.
3. Set the optional **Display Name** if you would like the server to appear in the server list with a name other than its **Server Name or IP Address**.
4. Enter the **Username** used to connect to the server.
5. If you would like to save your password so you don't have to enter it every time you connect, turn **Save Password** to **ON**.
    a. If you enable the **Save Password** option, a password window will appear. You will need to enter and confirm your password before it is saved.
6. When done configuring the new server, tap the **Save** button.

Connecting to a Server

You can connect to any server displayed in your **Servers** list. When you tap the server you want to connect to, you will be prompted for your password, if required.

Once connected, the shared volumes on the server will be displayed in the **Browse** pane. You can now navigate the shared volume.

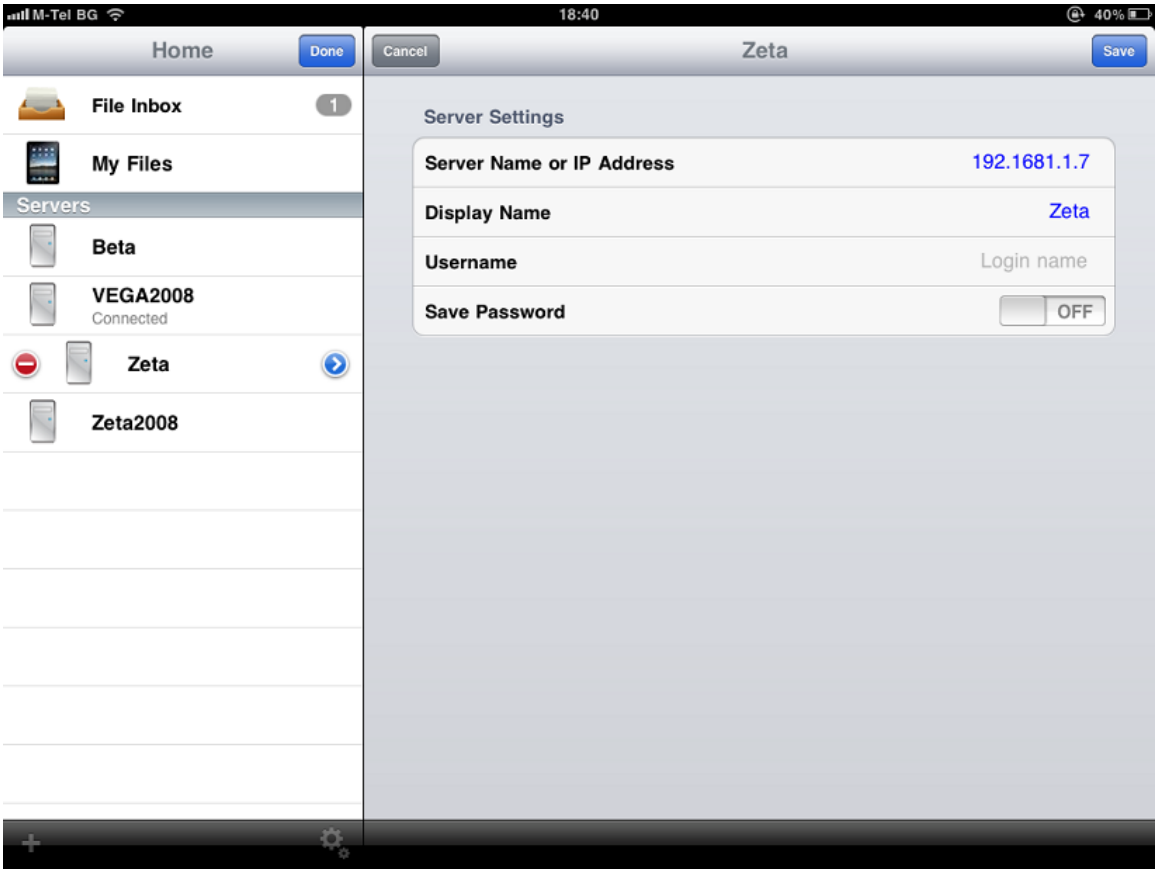
There is no need to manually disconnect from servers. Your connection will shut down when you leave the mobilEcho application. If your management profile settings allow you to save your password, servers will continue to be accessible when you later return to mobilEcho.

Editing Your Servers

If your ability to add and edit servers has not been disabled in your mobilEcho management profile, an **Edit** button will be available in the top bar of the **Home** pane. Only servers you have personally added to mobilEcho can be edited. Management assigned servers cannot be edited.

To modify server settings:

1. Tap the **Edit** button. A  sign will appear in front of the servers that can be edited.
2. Tap the  button to the right of the server you want to edit.
3. Make the needed changes on the right-hand pane and tap the **Save** button. For more information about the **Server Settings**, see Adding a New Server.
4. To exit the edit mode, tap the **Done** button on the **Home** pane.



Deleting an Existing Server

You can delete servers you have added to mobilEcho.

There are two ways to delete a server:

- By using the **Edit** button:
  1. Tap the **Edit** button.

2. Tap the  sign.
3. Tap the **Delete** button.
4. Tap **Continue** to confirm the delete.

- By swiping:
  1. Swipe your finger over the server you want to remove from your contact list.
  2. Tap the **Delete** button that appears next to it.
  3. Tap **Continue** to confirm the delete.

Configuring mobilEcho Client Management

Configuring mobilEcho Client Management

The settings and capabilities of the mobilEcho client application can be configured by your IT administrator using a client management profile. Your IT administrator may configure your mobilEcho servers so that you must have a client management profile in order to connect.

If you are enrolled in mobilEcho Client Management, some of your mobilEcho client application settings may be locked down and you may be limited to connecting only to the servers assigned by your profile. In many mobilEcho deployments, the only way to access your corporate mobilEcho servers will be to enroll your mobilEcho client in mobilEcho client management and accept these settings.

Server-side Management Policies

The mobilEcho client application can enroll in a corporate mobilEcho Client Management server which configures your mobilEcho client according to a specific client management profile. Depending on the management profile configured by the IT administrator, your mobilEcho client application may have different settings and features available.

The mobilEcho client application settings and features controlled by the management profile include:

- Require mobilEcho application lock password
- App password complexity requirements
- Ability to remove mobilEcho from management
- Allow emailing and printing files from mobilEcho
- Allow storing files on the device
- Allow mobilEcho on-device files to be included in iTunes backups
- Allow sending files to mobilEcho from other applications
- Allow opening mobilEcho files in other applications
- Restrict the other applications that mobilEcho files are allowed to be opened into
- Allow PDF annotation
- Allow file and folder creation, renames and deletes
- Allow moving files
- Require confirmation when deleting
- Servers, folders, and home directories can be assigned so they automatically appear in the mobilEcho

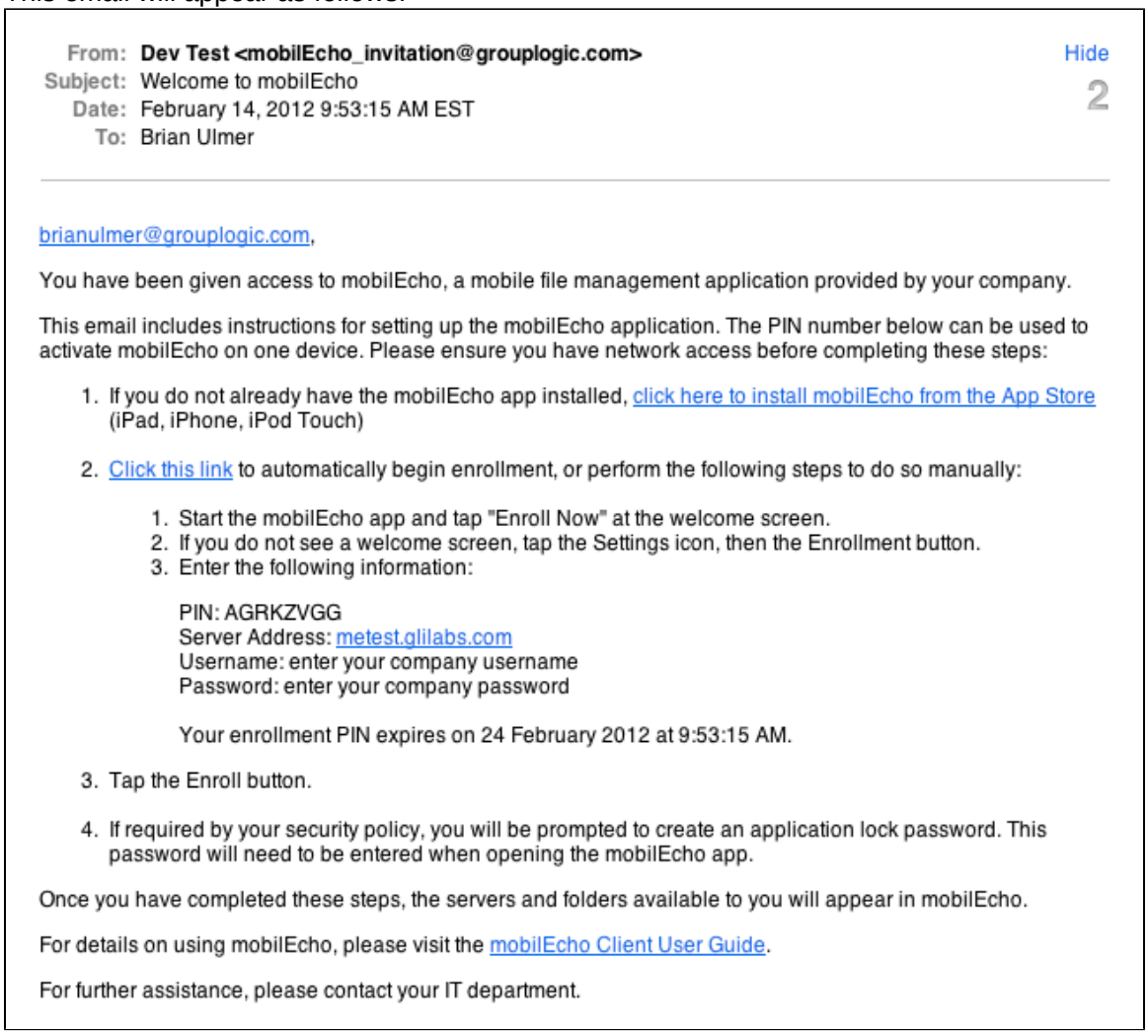
client app
- Assigned folders can be configured to perform 1-way to 2-way syncing with the server

Enrolling the mobilEcho app in mobilEcho Client Management

To enable you to enroll your mobilEcho client application in client management, your IT administrator can send you a management invitation email. This email will include enrollment instructions and some necessary information, including:

- A link to install mobilEcho from the Apple App Store
- A link to launch mobilEcho and automatically start the enrollment process
- A one-time use PIN number (optional, depending on how the mobilEcho server is configured)
- The management server's address

This email will appear as follows:



From: **Dev Test <mobilEcho_invitation@grouplogic.com>** Hide
Subject: Welcome to mobilEcho
Date: February 14, 2012 9:53:15 AM EST
To: Brian Ulmer

2

brianulmer@grouplogic.com,

You have been given access to mobilEcho, a mobile file management application provided by your company.

This email includes instructions for setting up the mobilEcho application. The PIN number below can be used to activate mobilEcho on one device. Please ensure you have network access before completing these steps:

1. If you do not already have the mobilEcho app installed, click here to install mobilEcho from the App Store (iPad, iPhone, iPod Touch)
2. Click this link to automatically begin enrollment, or perform the following steps to do so manually:
    1. Start the mobilEcho app and tap "Enroll Now" at the welcome screen.
    2. If you do not see a welcome screen, tap the Settings icon, then the Enrollment button.
    3. Enter the following information:

        PIN: AGRKZVGG
        Server Address: metest.glilabs.com
        Username: enter your company username
        Password: enter your company password

        Your enrollment PIN expires on 24 February 2012 at 9:53:15 AM.
3. Tap the Enroll button.
4. If required by your security policy, you will be prompted to create an application lock password. This password will need to be entered when opening the mobilEcho app.

Once you have completed these steps, the servers and folders available to you will appear in mobilEcho.

For details on using mobilEcho, please visit the mobilEcho Client User Guide.

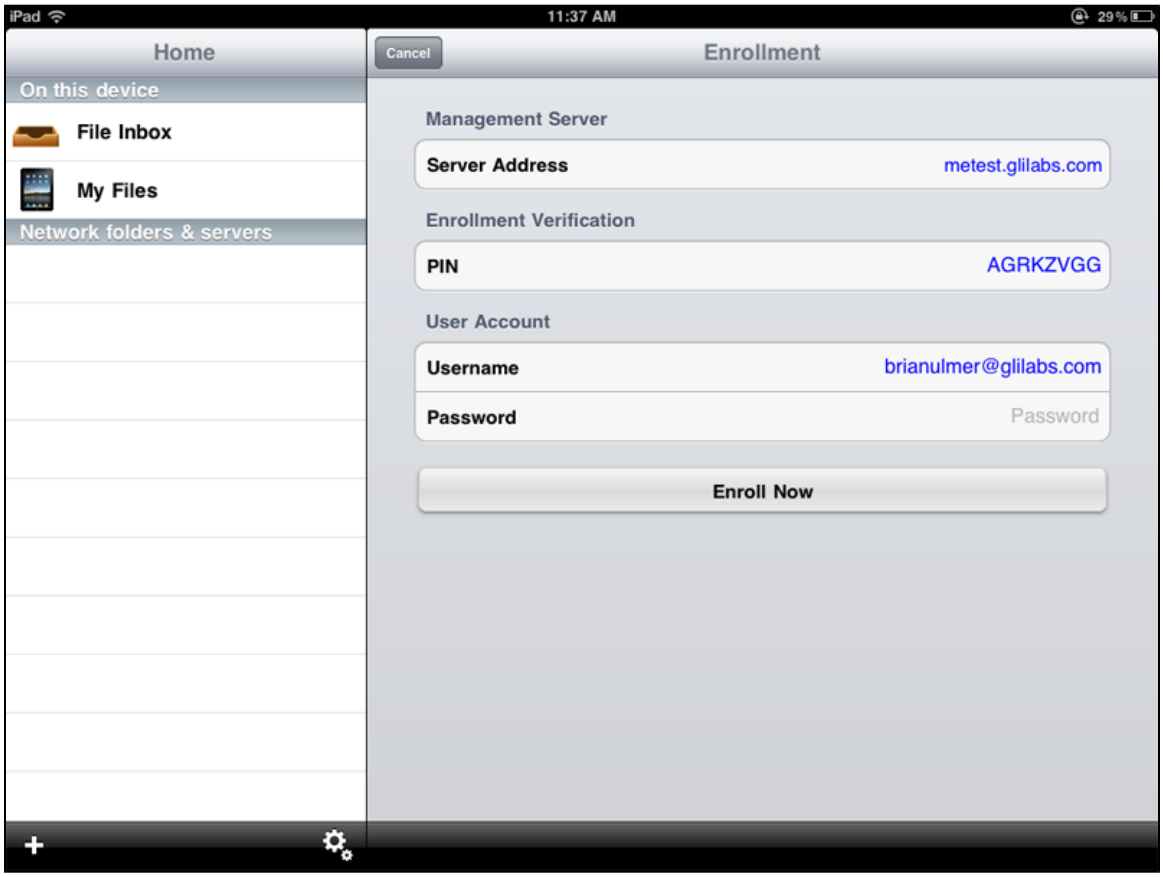
For further assistance, please contact your IT department.

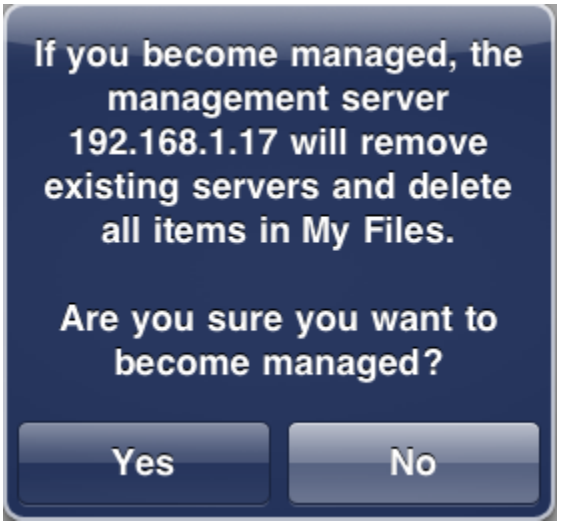
To enroll in client management, follow the steps below:

1. Open the email sent to you by your IT administrator and tap the "**click here to install mobilEcho**..." link if you have not yet installed mobilEcho.
2. Once mobilEcho is installed, return to the invitation email on your device and tap "**Click this link to automatically begin enrollment**..." in step 2.

> ⚠ Currently, when using the Outlook Webmail (OWA) to Enroll a user, the enrollment link will not work. Instead, it will open another OWA website within.

   a. If you do not have email on your device, or if your IT administrator has given you your enrollment **Server Address** and **PIN** by another means, follow the steps within step 2 in the email example above to manually start mobilEcho and perform enrollment.
3. An enrollment form will be displayed. If you used the link in the invitation email to start the enrollment process, your **Server Address**, **PIN**, and **Username**will be automatically filled out. If they were not, please enter these items.
   a. If your server does not require a **PIN** number, it will not be displayed in the enrollment form.
4. Enter your password and tap **Enroll Now**to continue.
   a. Note that the **Username** and **Password** are your standard company username and password. This is likely the same as you use to log into your computer or to your email.
5. After completing the entire form, tap the **Enroll** button.
6. Depending on the configuration of your company's server, you may be warned that your management server's security certificate is not trusted. To accept this warning and proceed, you can click **Proceed Always**.
7. If a mobilEcho application lock password is required, you will be asked to set one. Password complexity requirements may apply and will be displayed if needed.
8. A confirmation window may appear if your management profile restricts the storage of files in mobilEcho or disables your ability to add individual servers from within the mobilEcho app. If you have files stored locally in the mobilEcho app, you will be asked to confirm that any files in your **My Files** local file storage will be deleted. If you select **No**, the management enrollment process will be canceled and your files will remain unchanged.





Automatically assigned servers, folders, and your home directory may be added to the mobilEcho application **Network folders & servers** list after accepting the management profile. Synchronized folders may be added to your **On this device** list. Depending on the management profile, the mobilEcho client may be limited to connecting only with the assigned servers and folders.

Removing Management Profile

There are two options to remove your mobilEcho client from management:

- Turn Off the **Use Management** option (if allowed by your profile)
- Remove the mobilEcho client application

Depending on your management profile settings, you may have the right to remove the mobilEcho client from management. This will likely result in you not being able to access corporate files servers. If you are allowed to do so, follow these steps to unmanage your device:

1. Tap the **Settings** menu.
2. Turn **OFF** the **Use Management** option.
3. Your profile may require that your mobilEcho client data is wiped when removing the device from management. You can cancel the process at this point if you don't want to be wiped.
4. Confirm removing mobilEcho from management by tapping **YES** in the confirmation window.

If your mobilEcho management profile does not allow you to unmanage your client, the **Use Management** option will not be displayed on the **Settings** menu. In this case the only way to remove the device from management is by uninstalling the mobilEcho application. Uninstalling the mobilEcho application will erase all existing mobilEcho data and settings and will return the user to default application settings after reinstalling.

To uninstall the mobilEcho app, follow the steps below:

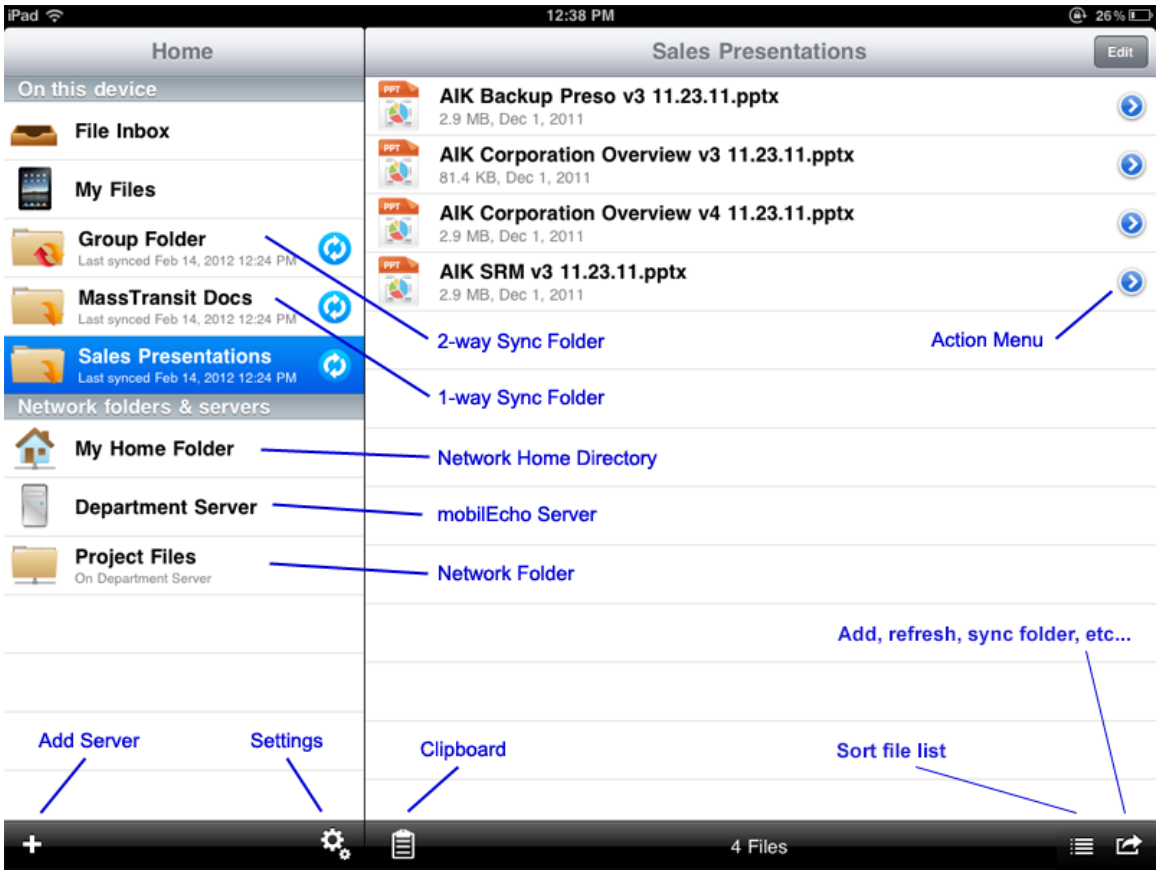
1. Hold your finger on the mobilEcho client app icon until it starts shaking.
2. Tap the "**X**" button on the MobilEcho application and confirm the uninstall process.
3. To reinstall the mobilEcho client app, visit http://www.grouplogic.com/web/meappstore

Application User Interface Overview

Main Window Overview

The main window of the mobilEcho client application consists of two panes: **Home** and **Browse**.

If your mobilEcho application is managed by a mobilEcho client management profile, this window may be missing some options that would normally be available when not managed.



Main Window Layout and Buttons

Home navigation pane -- Contains all the file sources available in mobilEcho.

Edit button in **Home** menu bar – Use to edit servers you have added to mobilEcho. This option may not be visible if your mobilEcho client has a client management profile that disables the ability to add servers manually.

On this device list -- All the files and synchronized folders that are stored on your device.

- **File Inbox** – Contains any files you've sent to mobilEcho from other applications, using the other application's **Open In** command. From the other application, choose **Open in mobilEcho** and the file will be automatically transferred to the mobilEcho **File Inbox**, where it can be easily located and moved to a server location, or to **My Files** for local storage.

- **My Files** – Contains files you choose to store locally on your iPad. Any files in **My Files** are available at all times, even when you're not connected to a network. Copy or move files here for offline use. Sub-folders can be created to organize your files, just like on a computer.
- **1-Way Sync Folder** -- This is a folder that is synced from the server to your device only. It is a read-only folder that is updated any time files change on the server. You will always be able to access these files, even when you do not have a network connection.
- **2-Way Sync Folder** -- This is a folder that is initially synced from the server to your device. After the initial sync, any changes made to files on your device will be synced to the server, and any changes made to files on the server will be synced back to your device. These files are also available even when you do not have a network connection. Any changes made to these files while you are not connected will be synced to the server the next time you have a network connection.

Network folders and servers list – All servers, folders, and home directories that have been added to mobilEcho are shown in this section of the **Home** menu. These items are only accessible when you have a network connection.

- **Network Home Directory** -- This is typically the same network home directory that you have access to from your Mac or PC. You can add files to your home directory from your computer and then access them at any time from mobilEcho on your device.
- **mobilEcho Server** -- All servers listed give you access to any file shares on that server that you have permission to access.
- **Network Folder** -- These are specific folders on a mobilEcho server, giving you direct access to individual file shares or specific folders within file shares.

Add Server button – Use to add new servers to your **Servers** list. This option may not be visible if your mobilEcho client has a client management profile that disables the ability to add servers manually.

Settings button – Use to verify or change application settings or to access help information.

Browse pane – The right-hand side **Browse** pane allows you to browse files and folders and work with them.

Edit button in **Browse** menu bar – Use to select multiple files for copying, moving or deleting.

Search box – Use to search for files. You may see options for choosing to search the current folder or the entire shared volume, and for choosing to search by file name or file contents, depending on your server configuration.

Action Menu – Used to select the action you would like to perform with the file or folder.

Clipboard – Used in the process of moving or copying files. The clipboard shows the file transfer status during a copy or move. For further details, see the next section on this page, Clipboard Overview.

Refresh -- Pull down on the files list in the right-hand **Browse** pane to refresh the files list. If files are added to a folder that you are already viewing, refreshing the folder will update the folder and show the new files.

Add, refresh, sync folder button – Use to create a new folder in the current folder being browsed, to copy files from your iPad photo library into the current folder, refresh this files list, to add the current folder to your local files as a sync folder, to email a link to the current folder, or to rename the current folder being browsed.

Location Services Prompt

When you first use the **Copy Photos** feature in the **Add to Folder** menu, your iPad will ask you to allow mobilEcho to know your current location. This is done because photos taken with the iPad are typically tagged with the location the picture was taken, and moving them to mobilEcho will move that embedded location data along with the photo. mobilEcho does not independently record your location in any way, nor does it access the GPS / location services on your device.

Clipboard Overview

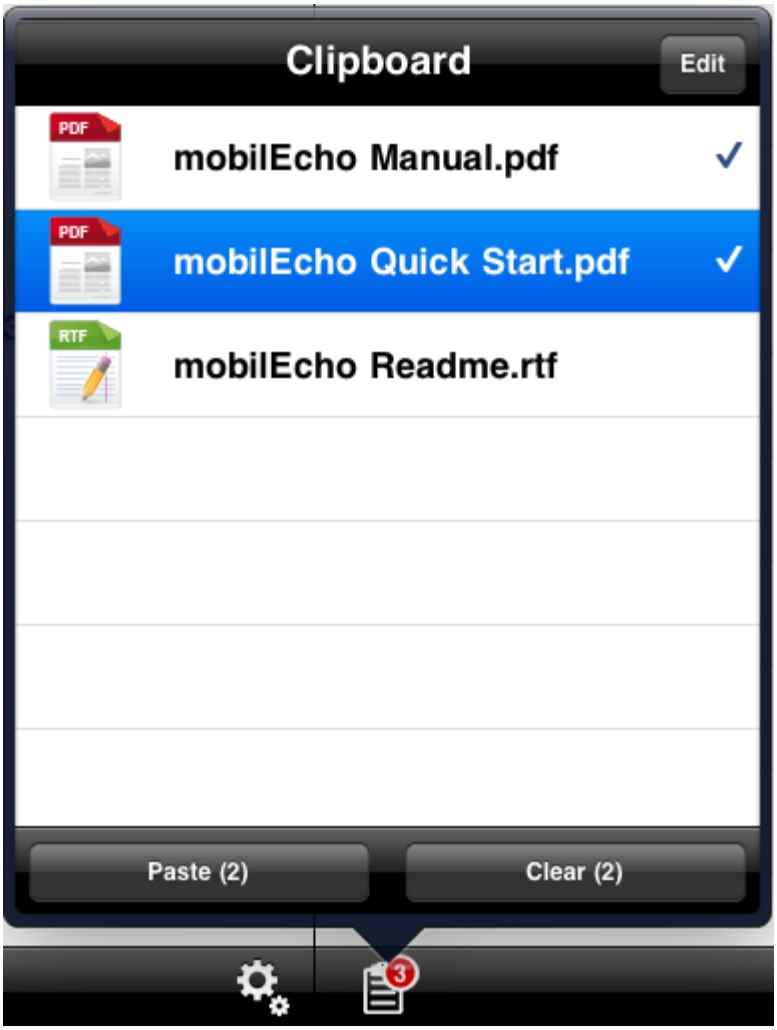
When you chose to copy or move files they will first appear on the clipboard. The clipboard allows you to select the item(s) you'd like to copy or move, and then navigate to the desired destination folder and paste them. The clipboard appears when you tap the **Clipboard** icon.

To copy a file, tap the file and select **Copy with Clipboard** from the file's action menu.

To move a file, tap the file and select **Move with Clipboard** from the file's action menu.

NOTE

The mobilEcho client application clipboard works like a computer clipboard. If you copy files with the clipboard and have not get pasted them, then you select another set of files and copy them with the clipboard, the previously copied files will be cleared and replaced with the new file(s). No files are actually copied or moved unless you choose to paste them.



Clipboard Actions

Paste – use to copy or move the selected files in the current directory.

- Tap **Paste All** – if you would like to paste all files stored in the clipboard at once.
- You can also tap the individual files you would like to move. A checkmark will appear beside each selected file.
    - Then tap the **Paste** button to paste only the selected files. The non-selected files will remain in the clipboard.

Clear – use to remove files from the clipboard.

- Tap **Clear All** – if you would like to remove all files in the clipboard.
- You can also tap the individual files you would like to clear. A checkmark will appear beside each selected file.
    - Then tap the **Clear** button to clear only the selected files.

Edit – use the **Edit** button to select files you want to remove from the clipboard. This action does not delete the original file, it simply removes it from the clipboard, leaving it in its original location.

1. Tap the **Edit** button.
2. Tap the  sign.

3. Tap the **Clear** button for the file you want to discard.

Working with Files

Working with Files

The mobilEcho client application can preview, copy, move, rename, delete, print, email, and open files in other applications on the iPad. You can also annotate PDF files that are opened in the mobilEcho app.

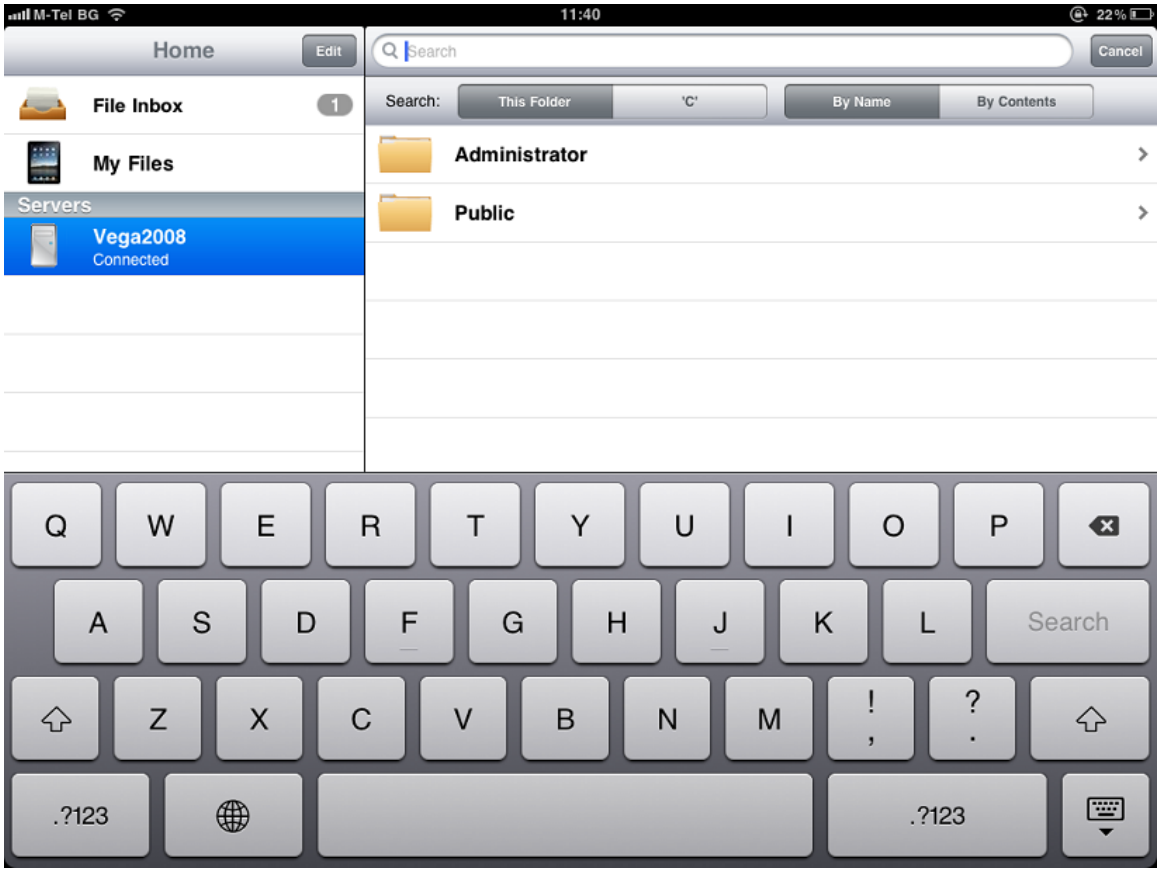
Searching For Files and Folders

mobilEcho allows you to easily search servers for the files you need. Searches are performed on the server-side, providing fast search results and minimizing bandwidth usage.

Searches can be performed on the currently browsed folder or on the entire shared volume being browsed. This is controlled by selecting either the **This Folder** button, or the shared volume button to its right. The shared volume button will display the name of the shared volume being browsed.

Two types of search can be performed:

- **By Name** - by default, mobilEcho searches for files and folders by name.
- **By Contents** - this option searches for files with the desired search term in their file contents. Search results will also include files and folders with the search term in their name.

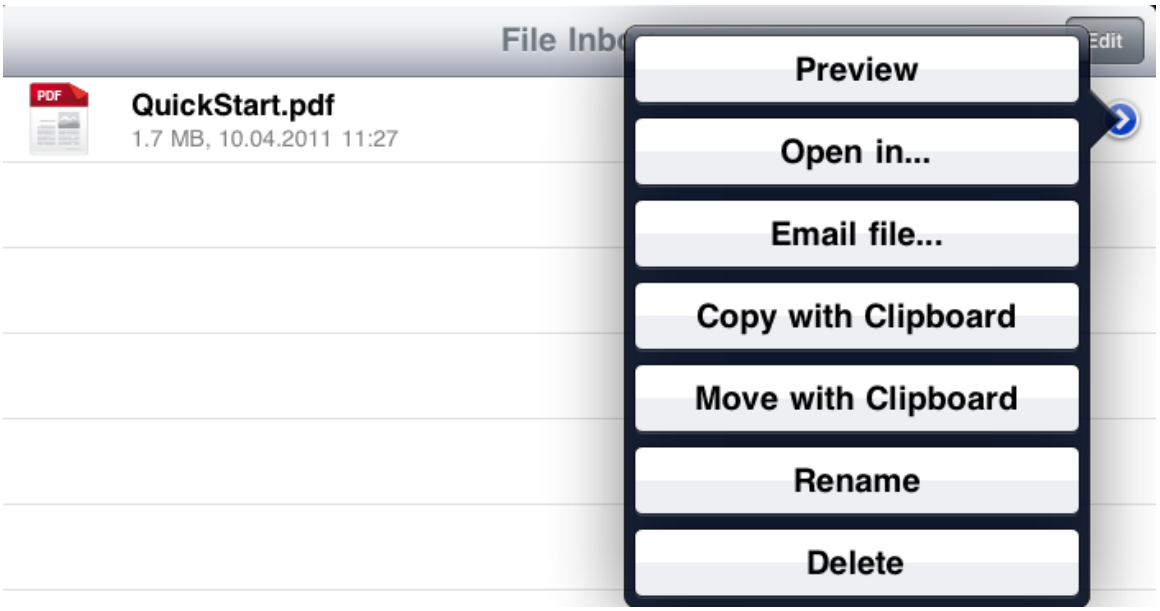


In order for **By Content** search to function, the mobilEcho server has to have Windows Search services running and configured to index the files being shared with mobilEcho. If your IT administrator has not installed Windows Search, you will only be able to search **By Name**.

Opening Files

When opening a file in mobilEcho you can preview the file or you can choose to open it in another application on the iPad.

- Tap the **Action Menu** button next to the desired file and select **Preview**to preview the file in mobilEcho. The preview option will open only file types supported by mobilEcho. If the MobilEcho application is not able to read the file, you may want to try opening it in another application.
    - **PDF Annotation** -- When you open a PDF file, you will see additional tools for adding annotations to the PDF. These include adding notes, text, highlights, strikethroughs, freeform drawing, etc. To perform PDF annotation, tap and hold to select text, or choose from the available PDF annotation tools in the top menu bar.
- Tap the **Open In...**option to open the file in another application on the iPad.
    - A menu will appear listing all available applications on your iPad that support opening the selected file type. Select the desired application.



Note:

Currently you can't preview password protected documents directly in mobilEcho. For password protected documents you should use **Open In…** and select an app which supports this.

File Operations

mobilEcho can copy, move, rename, and delete files. When doing a copy or a move, files can be transferred from server to server, from the iPad to a server or from a server to the iPad. For more information on copy and move with the clipboard see the Clipboard Overview section.

Folders cannot currently be copied or moved in mobilEcho. This capability will be added in a future release.

Add to Folder Options

mobilEcho can create new folders on servers and in the **My Files** local file storage area.

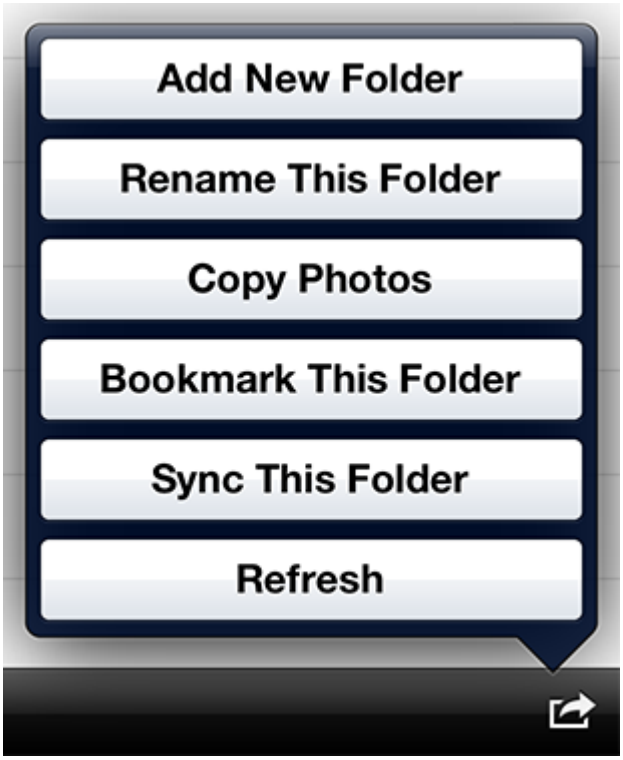
To create a folder within the folder you are currently viewing:

- Tap the **Add to Folder** button on the right end of the bottom menu bar.
- Select **Add New Folder**.

The **Folder Action Menu** contains additional options:

- **Rename This Folder** – Used to rename the folder you are currently browsing.
- **Copy Photos** -- Used to copy photos from the iPad photo library to folder you are currently browsing.
- **Bookmark This Folder** -- Create a shortcut to this folder.

- **Sync This Folder** – Sync the contents of this folder to your device for offline use. This can be done as a 1-way (server to device only) or 2-way sync.
- **Refresh** – Update the content of the folder to display the latest content from the server.

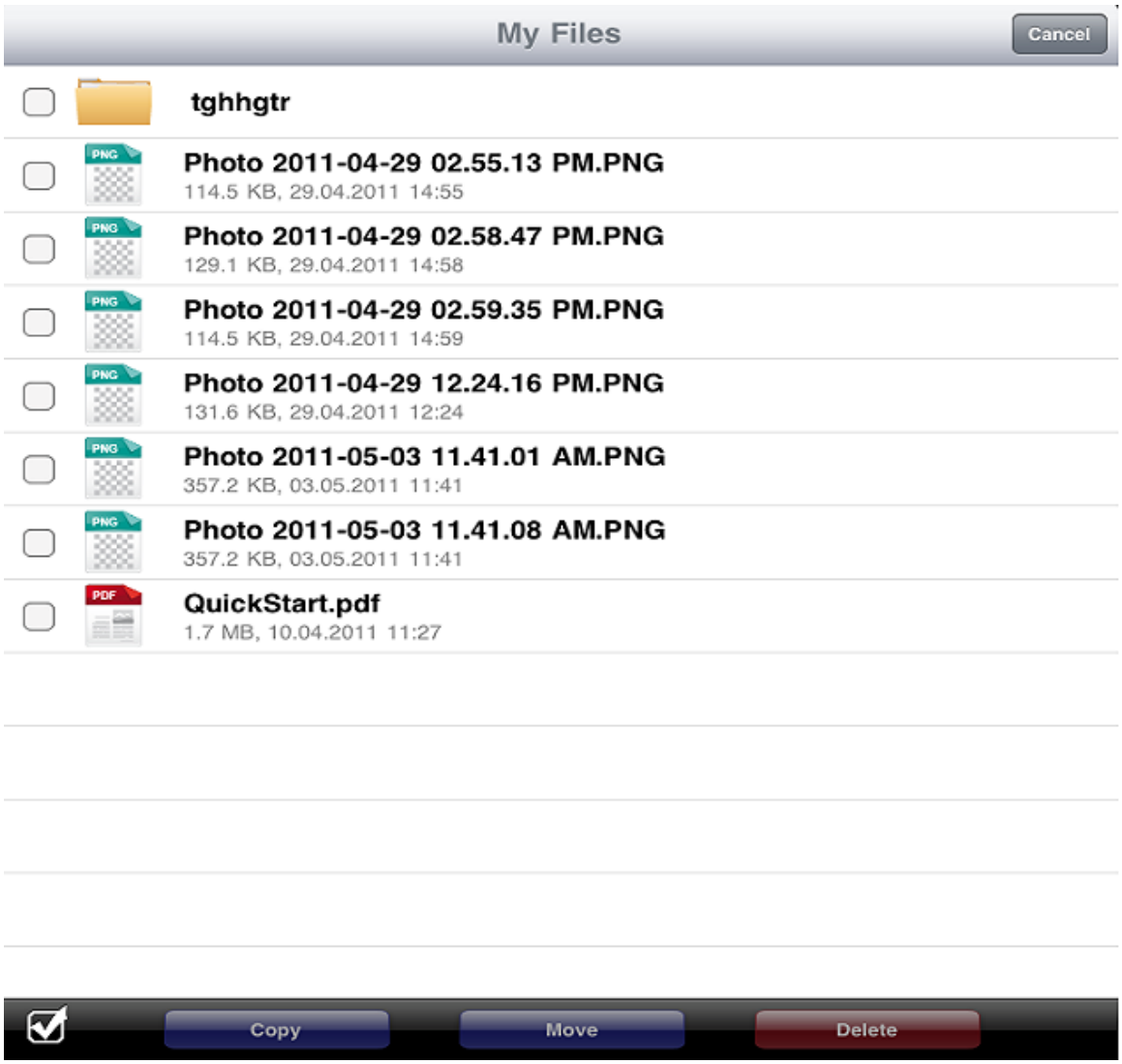


Edit Mode - Selecting Multiple Files

Use **Edit** mode to select multiple files to copy, move or delete.

1. Tap the **Edit** button on the **Browse** pane's top menu bar.
2. In the browse pane, select the desired files by tapping the box to the left of each file in the list.
    a. If you would like to select all available files in a particular folder, tap the **Select All** button. To unselect all files after they have been selected tap **Select All** again.
3. Tap the **Copy**, **Move** or **Delete** button, or use the **Cancel**button to exit Edit mode without making changes.

> **Note**
>
> mobilEcho does not currently support copying or moving folders. If you select a folder when using multi-select Edit mode, the copy and move buttons will be disabled.



Check Out and Check In of SharePoint Files

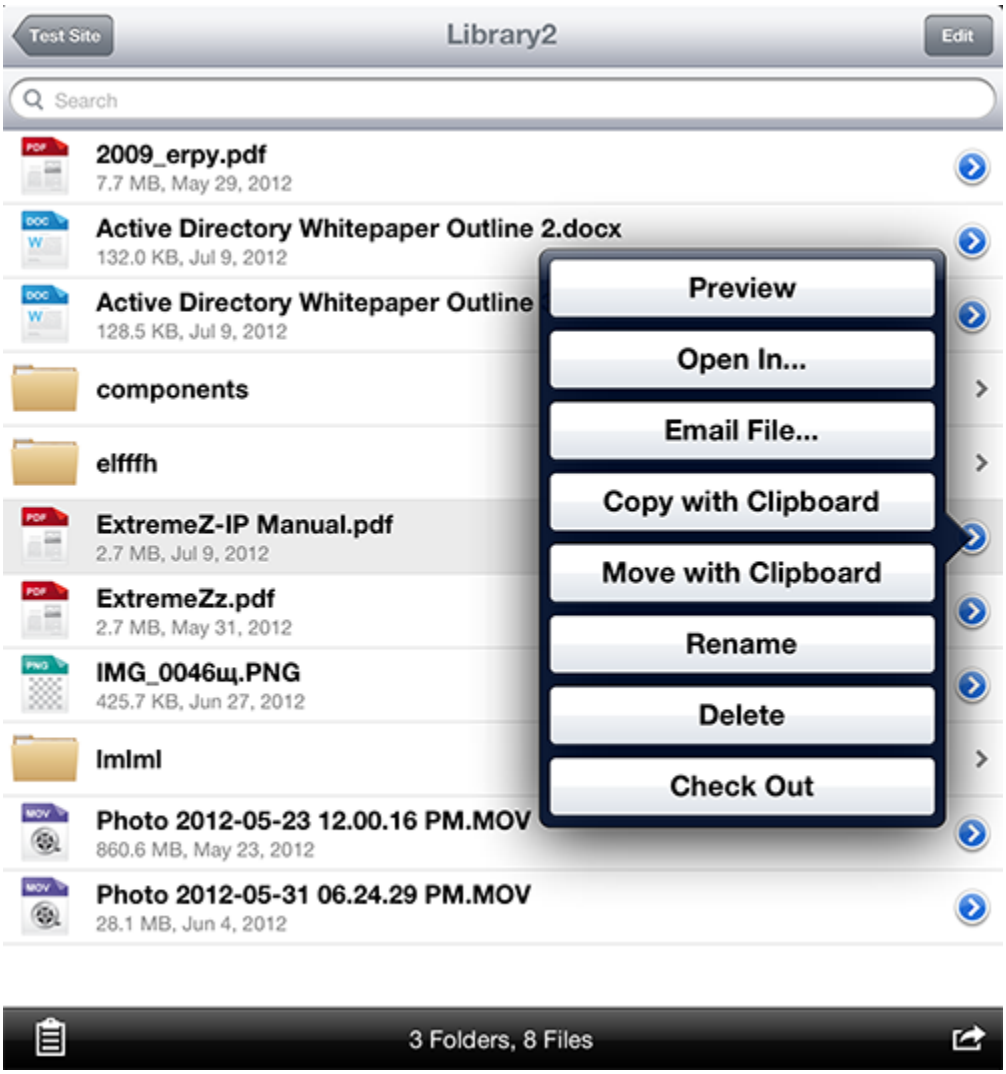
If mobilEcho is configured to provide access to files located on a SharePoint server, you will see three additional buttons available when you open the **Action Menu** for a file.

Check Out - Allows you to lock a file you plan to edit so that others do not also edit it at the same time. Once you **Check Out** a file, you can preview it and use PDF annotation or you can open it into another application for editing. Once the file has been edited, you will need to save it back into the folder it came from and overwrite the original file, in order to save your changes.

Check In - Allows you to unlock a file after you have edited it and saved it back to the server.

Discard Check In - Allows you to remove your Check Out without committing any changes to the file.

> **Note:**
>
> SharePoint 2007 doesn't allow the renaming of a checked-out file. It is allowed in SharePoint 2010.

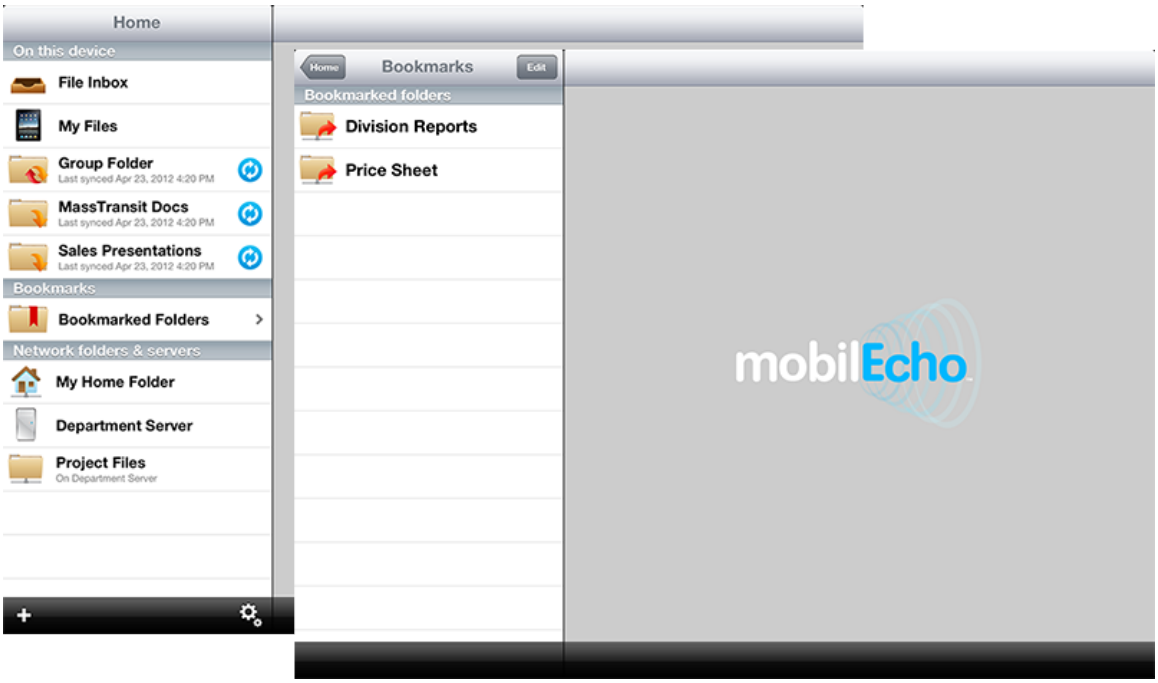


Bookmarking Folders

mobilEcho allows you to bookmark folders that you commonly use, so that you can quickly navigate to them in the future. These folders can reside within the local My Files storage area, within sync folders, or on a network server or folder. Bookmarks are shortcuts to their original folders, so a network connection will be required to access any bookmarked folders that reside in a network location.

To access your existing bookmarked folders:

- Tap the **Bookmarked Folders** item in the home menu.
- Next, tap the desired folder in the **Bookmarked folders** list to navigate to it.

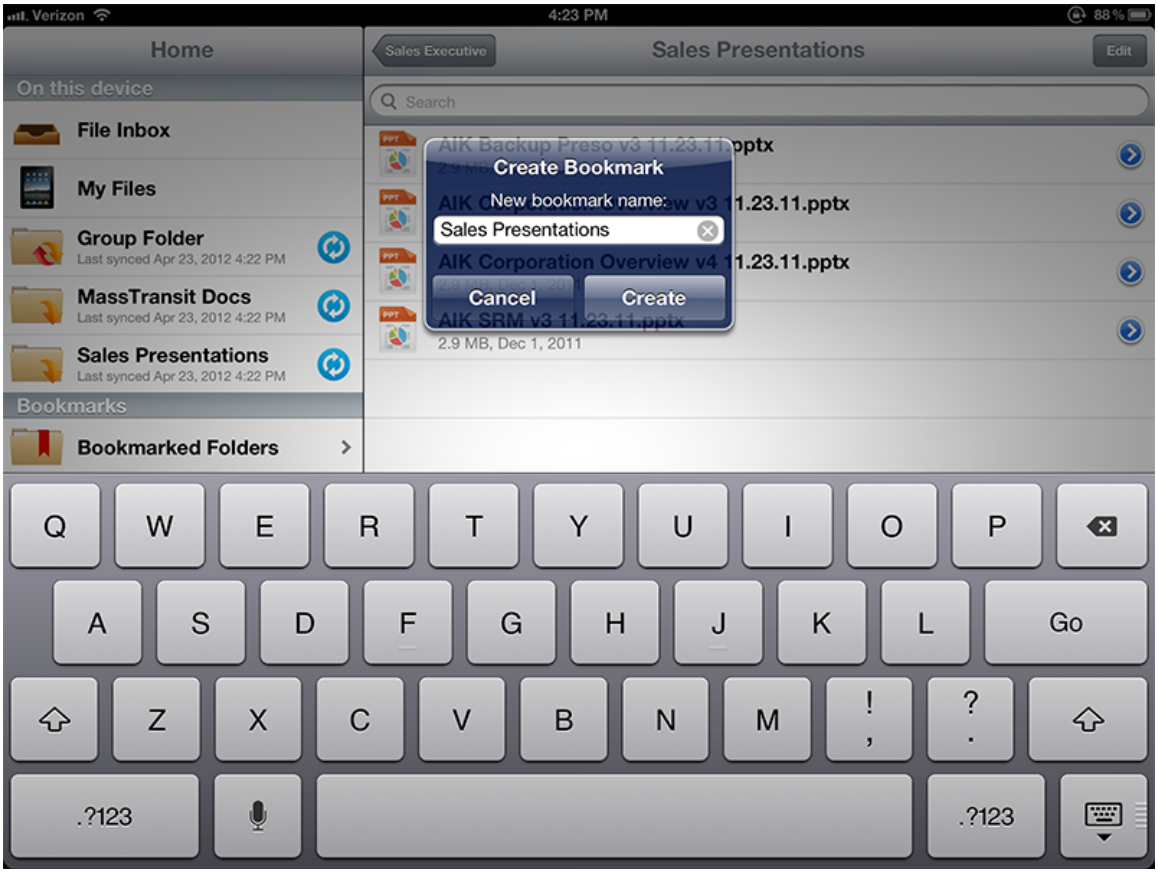


To bookmark a new folder:

- Navigate into the folder you would like to bookmark. In this example, we are bookmarking the **Sales Presentations** folder.
- Tap the **Folder Action Menu** and select **Bookmark This Folder**.

- Rename the bookmark, or accept the default name, and tap **Create**.

- The bookmark will now appear in the **Bookmarked folders** list.



To remove a bookmark using a swipe:

- Swipe across the bookmark you'd like to remove. A **Delete** button will appear.
- Tap the **Delete** button.

To remove a bookmark using the Edit button:

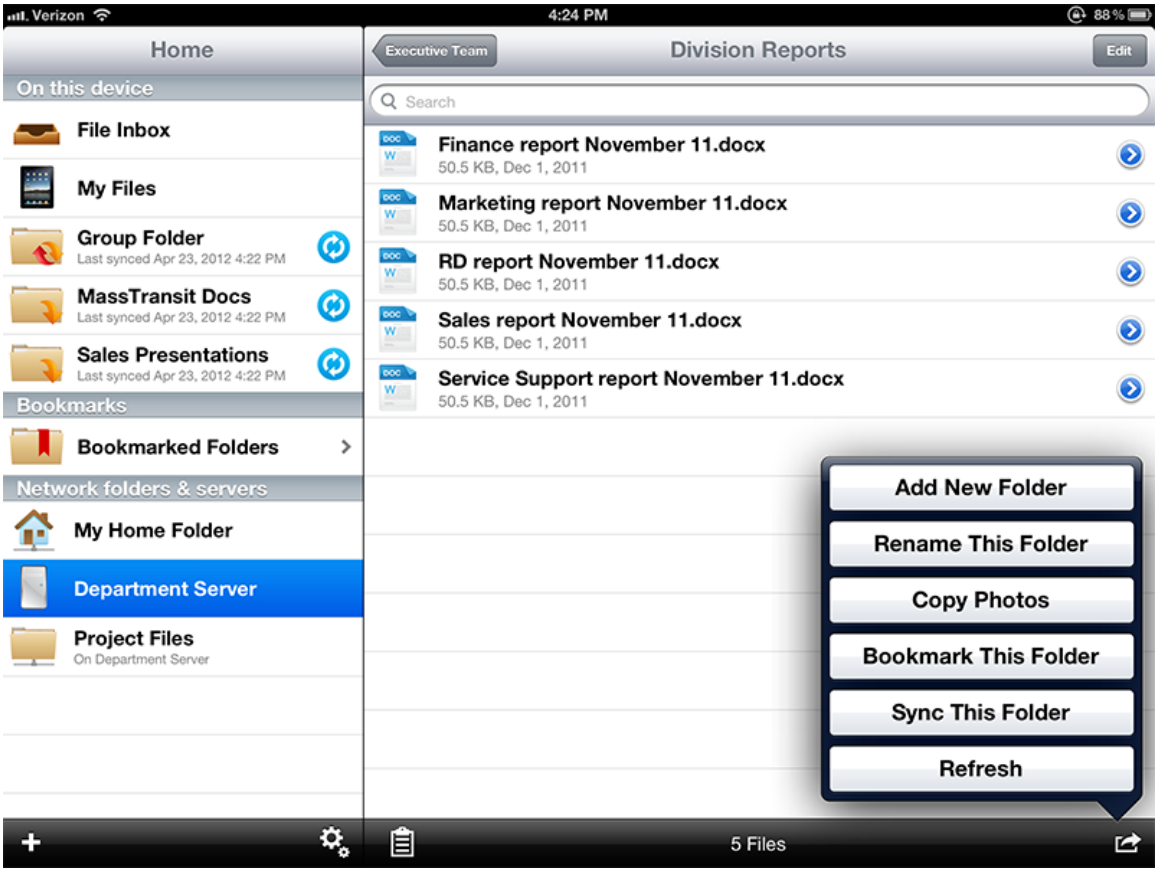
- Tap the **Edit** button at the top of the **Home** menu.
- All bookmarks will appear with a red 'minus' icon to the left of them.
- Tap the red 'minus' icon.
- Tap the **Delete** button.

Creating Sync Folders

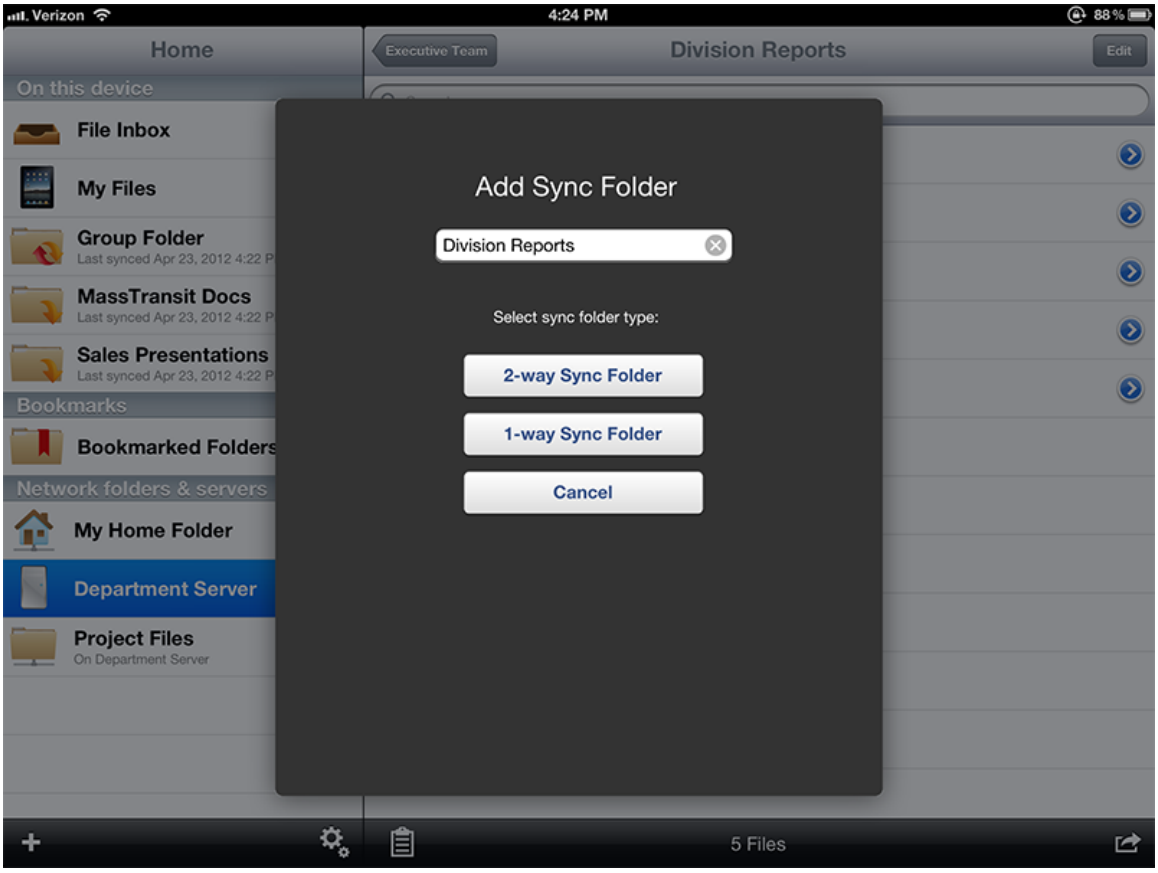
mobilEcho can sync network folders for storage on your device, within the mobilEcho app. This allows these folders and their contents to be accessed immediately without downloading files on-demand from the server, and ensures that these files are available, whether your online of offline.

To sync a folder:

- Navigate into the folder you would like to sync to your device. In this example, we are syncing the **Divisi on Reports** folder.
- Tap the **Folder Action Menu** and select **Sync This Folder**.



- The **Add Sync Folder** window appears,
- You can modify the **sync folder name**, or accept the default name.
- Choose the **sync folder type**:
    - **2-way Sync Folder** - Files are initially synced from the server to your device. Any changes made on the server-side or client-side are synced. Use this type of sync folder if you'd like to be able to edit files in the sync folder and have them sync back up to the server.
    - **1-way Sync Folder** - Files are only synced from the server to your device. Any changes made on the server-side will be automatically synced to your device. The files in this type of sync folder are read-only and cannot be modified from within the mobilEcho client app.



- The folder will appear in the **Home** menu.
- You will may be prompted to confirm the initial file sync operation before the folder's contents are synced.

You can remove any sync folders that you've added. Please note that sync folders automatically assigned to your mobilEcho app by your mobilEcho management profile can only be removed by your IT administrator. Removing a sync folder deletes the synced content from your device only, the corresponding folder on the server and all files within that folder will not be changed or deleted from the server.

To remove a sync folder using a swipe:

- Swipe across the sync folder you'd like to remove. A **Delete** button will appear.
- Tap the **Delete** button.
- Tap **Continue** at the **Confirm Delete** dialog to remove the sync folder.

To remove a sync folder using the Edit button:

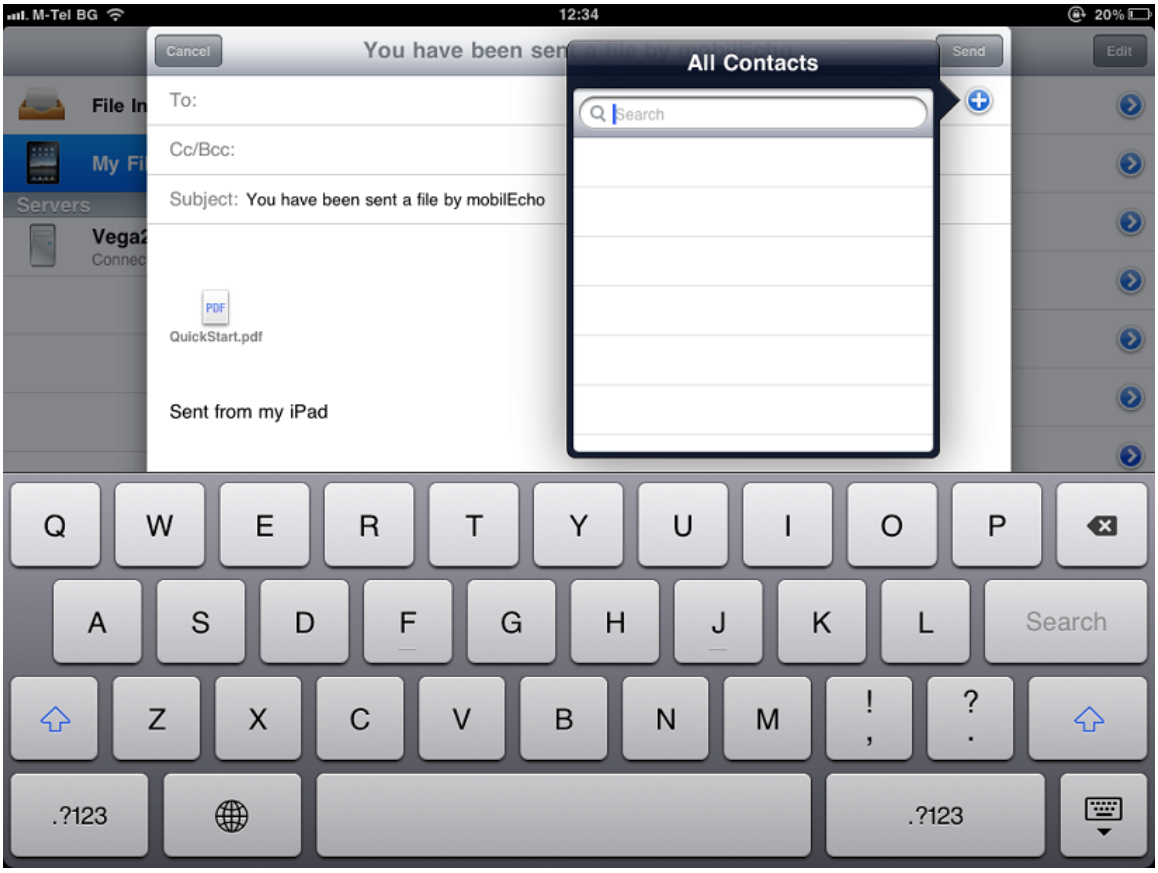
- Tap the **Edit** button at the top of the **Home** menu.
- All user-created sync folders will appear with a red 'minus' icon to the left of them.
- Tap the red 'minus' icon.
- Tap the **Delete** button.
- Tap **Continue** at the **Confirm Delete** dialog to remove the sync folder.

Emailing Files

To email files from the MobilEcho application:

1. Tap the **Action menu** of the file you want to send and select the **Email File...** option.
2. An email message window will appear. mobilEcho uses the email accounts that are configured in your iPad email app.
3. Specify a To: email address.
4. You can modify the Subject or add text to the body of the message if you wish.
5. To send the email, tap the **Send**button.

> **Client Management Regulation of Emailing Files**
>
> If your mobilEcho client has a management profile, it is possible your IT administrator has disabled mobilEcho's email capabilities. In this case, you will not see an **Email File...** button in the Action Menu.



Sending Files from Other Applications to mobilEcho

The mobilEcho application allows files from other iPad applications to be sent to mobilEcho. This is done using the **Open In** feature of the other application and choosing **Open in mobilEcho**. When a file is transferred from another application to mobilEcho, the file will appear in the **File Inbox**. Files in the **File Inbox** area can be moved or copied to a server or to the **My Files** area. Files stored in the **My Files** area can be accessed at any time, even when you are not connected to the network.

> **Availability of Open In**
>
> Some applications have not yet implemented the iOS Open In feature, which allows files to be sent to other applications. If your favorite app is missing **Open In**, we encourage you to send the developer feedback requesting the functionality.

Quickoffice Save Back Integration

The mobilEcho application has support for Quickoffice's "Save Back" feature, which allows users to save files back to the source they opened them from.

In order to **Save Back** files from Quickoffice to mobilEcho, the desired file must first be opened into Quickoffice using the mobilEcho application.

To do so follow these steps:

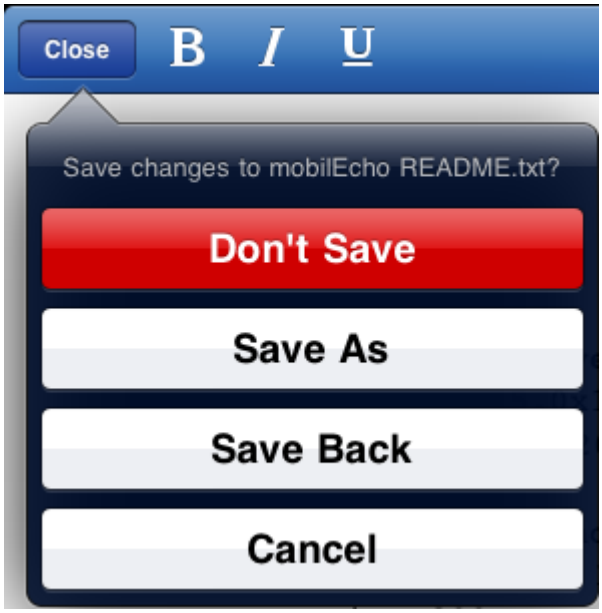
1. In the mobilEcho application tap the **Action Menu** button next to the desired file.
2. Select the **Open In...** option, and then select **Quickoffice**.

The file will now open in the Quickoffice application and the **Save Back** function will be available.

> **Creating new documents with Quickoffice**
>
> Quickoffice does not support the generic iOS **Open In** feature. Therefore, you cannot create a new file directly within Quickoffice and save it directly into mobilEcho. In this case the file didn't originally come from mobilEcho, so the **Save Back** function will not be available.
>
> If you need to create new documents in Quickoffice and store them in mobilEcho, we recommend you create blank Word, Excel, and Powerpoint document files and store them in a folder within mobilEcho. To create a new document, use the mobilEcho **Open In** featur e to open one of these blank template files into Quickoffice. Edit the file as necessary, and when you **Save Back** to mobilEcho, choose the **Rename and Save** option to save the file with a new name instead of overwriting the template.

To **Save Back** the file to mobilEcho:

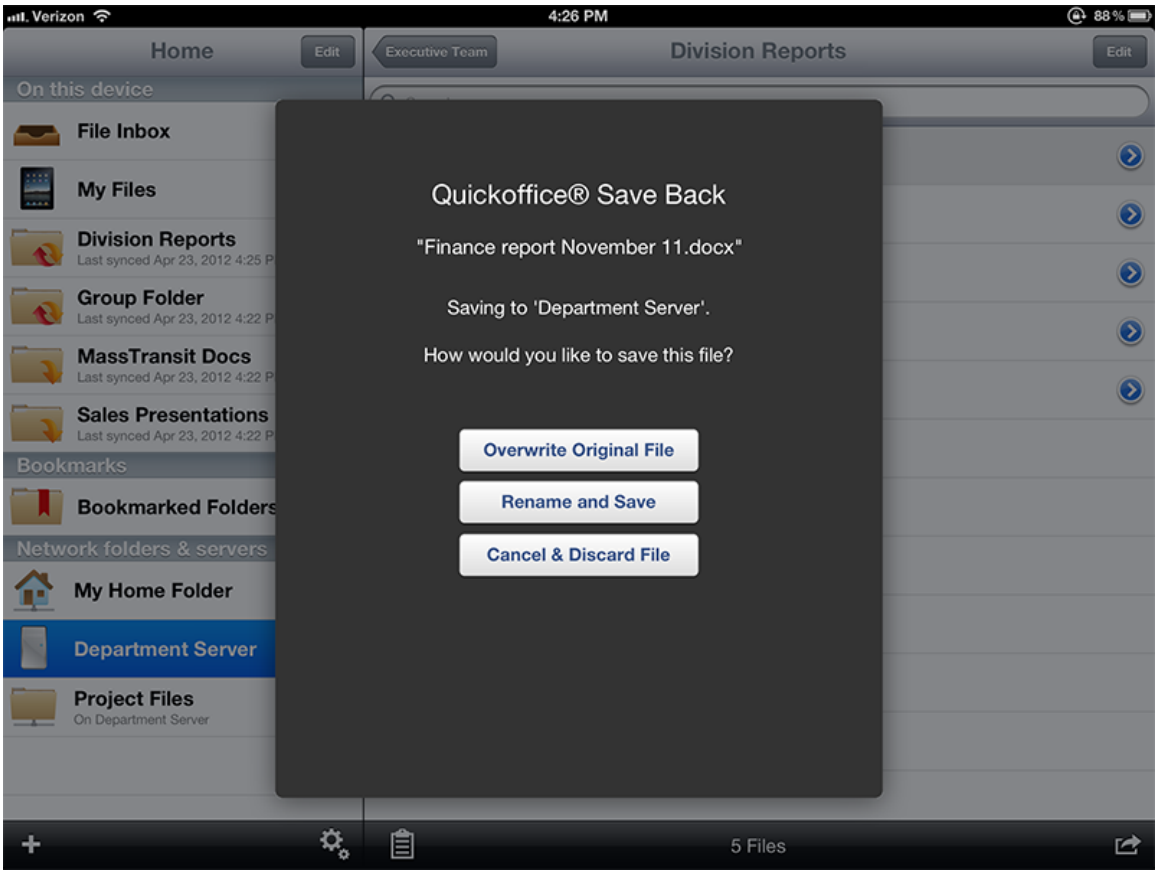
1. When you have finished editing your file in Quickofffice, tap the **Close** button.
2. In the menu that appears, tap the **Save Back** button.



3. A menu will appear listing only the mobilEcho application. Select **mobilEcho**.
4. mobilEcho will automatically start. You will be asked to enter your **App Password**, if one is configured.
5. Save Back will attempt to save the file directly into the location it was opened from. If that was a network location and you are no longer online, you will be asked if you'd like to save the file into the File Inbox instead. The file will be stored in the File Inbox on your device and you can move it back to a network location the next time you are online.
6. When prompted, you may choose to:
    a. **Overwrite Original File** - The copy of the file you originally opened into Quickoffice and edited will be overwritten with the new version. The original version will no longer exist. If the original file was modified by someone else while you were editing it, you will be warned and may choose to save the file with a new name instead.
    b. **Rename and Save** - You will be prompted to give the file you are saving a new name. The

original version will remain unchanged.

c. **Cancel & Discard File** - This will abort the saving of this file. Any changes to the file that were made will be lost. Quickoffice automatically closes the file when you **Save Back**, so you cannot return to the edited file by going back into the Quickoffice app.



Security Features

- Password Protection
- HTTPS Encrypted Network Communication
- Apple Data Protection

Password Protection

The mobilEcho client application can be configured to require authentication upon startup. This option prevents someone using your device from accessing mobilEcho without authorization.

Application password protection can be enabled on the mobilEcho **Settings** menu, or may be enabled automatically if you are managed by a mobilEcho management profile. For more information about creating an application password see Setting an Application Password.

In addition to the application lock password, mobilEcho uses your corporate Active Directory account to regulate access to all mobilEcho file servers.

HTTPS Encrypted Network Communication

The mobilEcho uses HTTPS protocol for all network communication. This ensures secure authentication

and file transfer between mobilEcho clients and servers. The HTTPS protocol encrypts all files during their transfer.

Apple Data Protection

All files within the mobilEcho application's storage area on the device are encrypted with Apple Data Protection, if Apple Data Protection is enabled.

To enable Apple Data Protection, you must have an iOS Passcode Lock set on your device.

To configure a passcode for your device:

1. Tap **Settings** > **General** > **Passcode Lock**.
2. Tap **Turn Passcode On** and follow the prompts to create a passcode.

Once a Passcode Lock is set up, Apple Data Protection will be automatically supported by iOS. If you later remove this passcode, your files will no longer be encrypted.

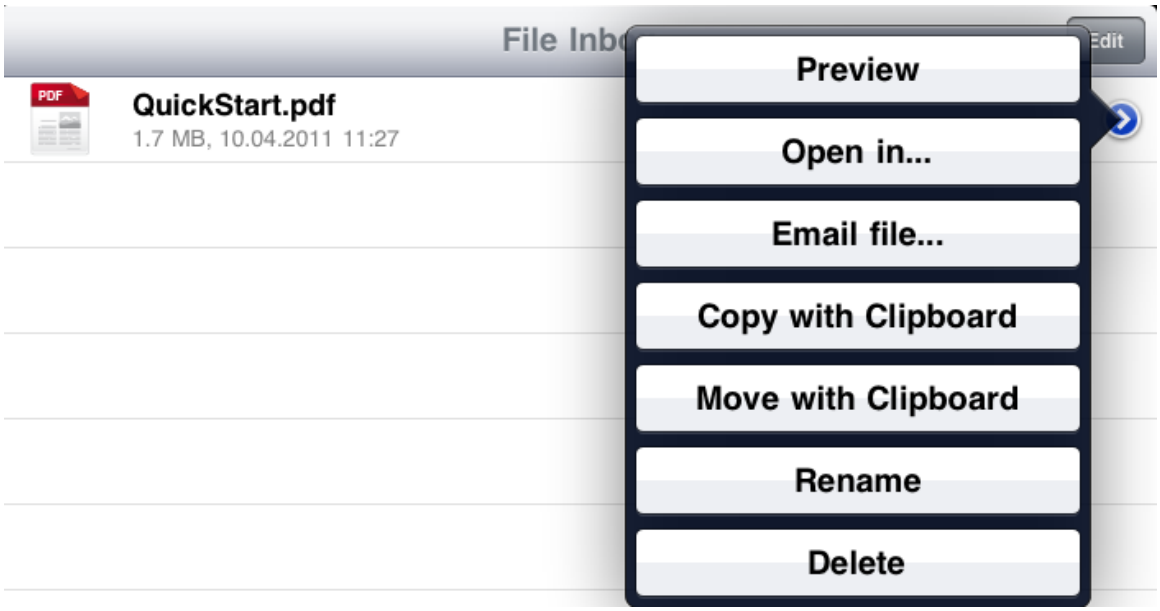
PDF Annotation

Opening PDF files for annotation

mobilEcho allows you to perform PDF annotation on PDF files opened in the mobilEcho app.

To open a PDF file:

1. Navigate to the file in mobilEcho.
2. Tap the file **Action Menu** and select **Preview**.



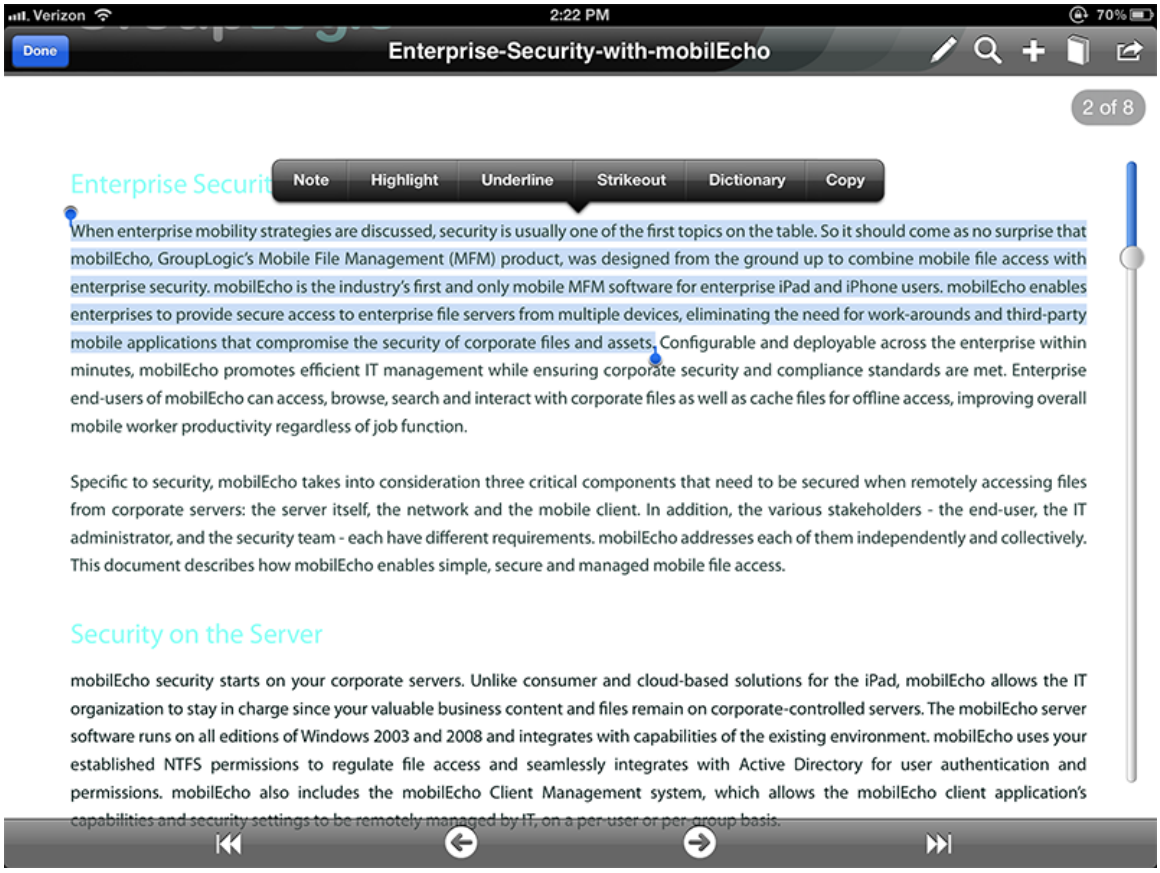
3. The file will open and PDF annotation icons will be displayed on the right hand side of the top menu bar.

Creating annotations

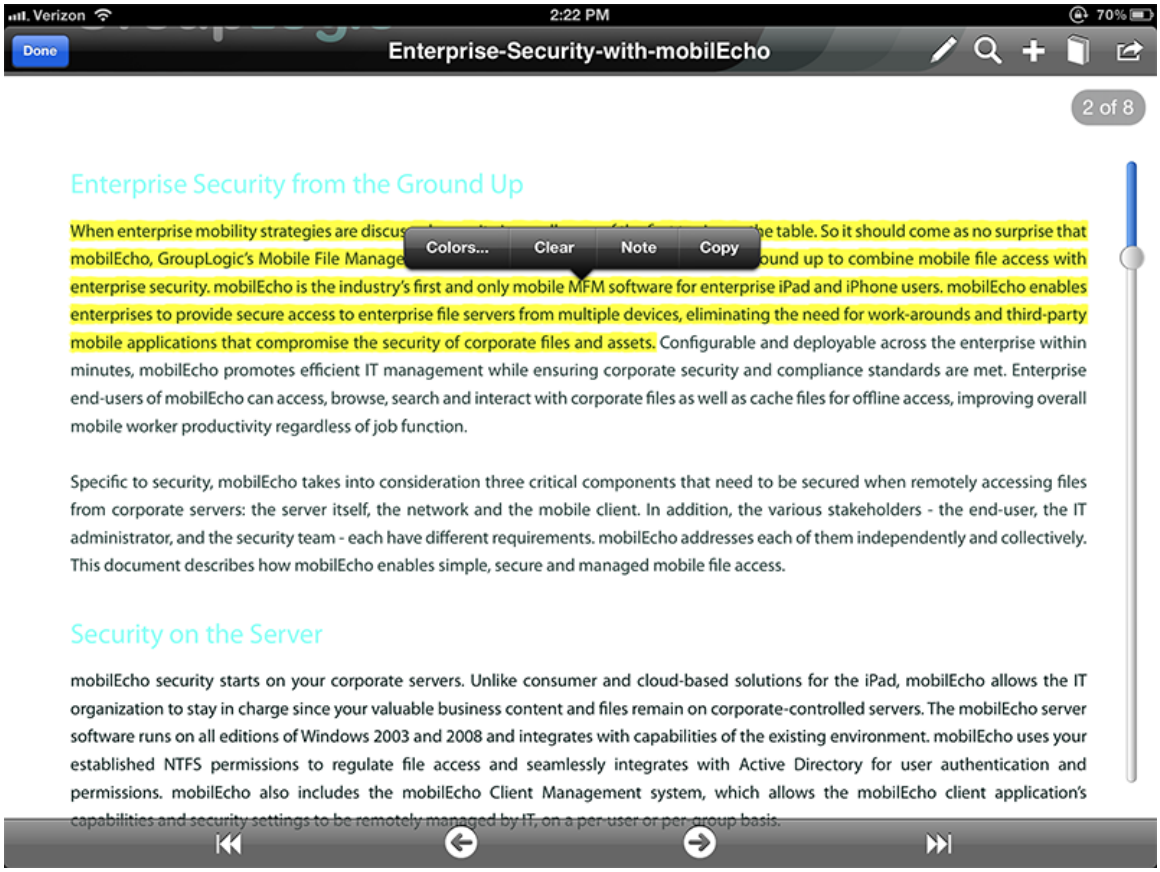
mobilEcho allows many types of PDF annotation to be added to a PDF file.

Add a Note, Highlight, Underline, or Strikeout to selected text

1. Tap and hold existing text within the PDF file.
2. A text selection tool appears.
3. Adjust the text selection to include the text you would like to annotate.
4. Tap the menu selection to choose the type of annotation you would like to add. In this example, we are adding a **Highlight**.



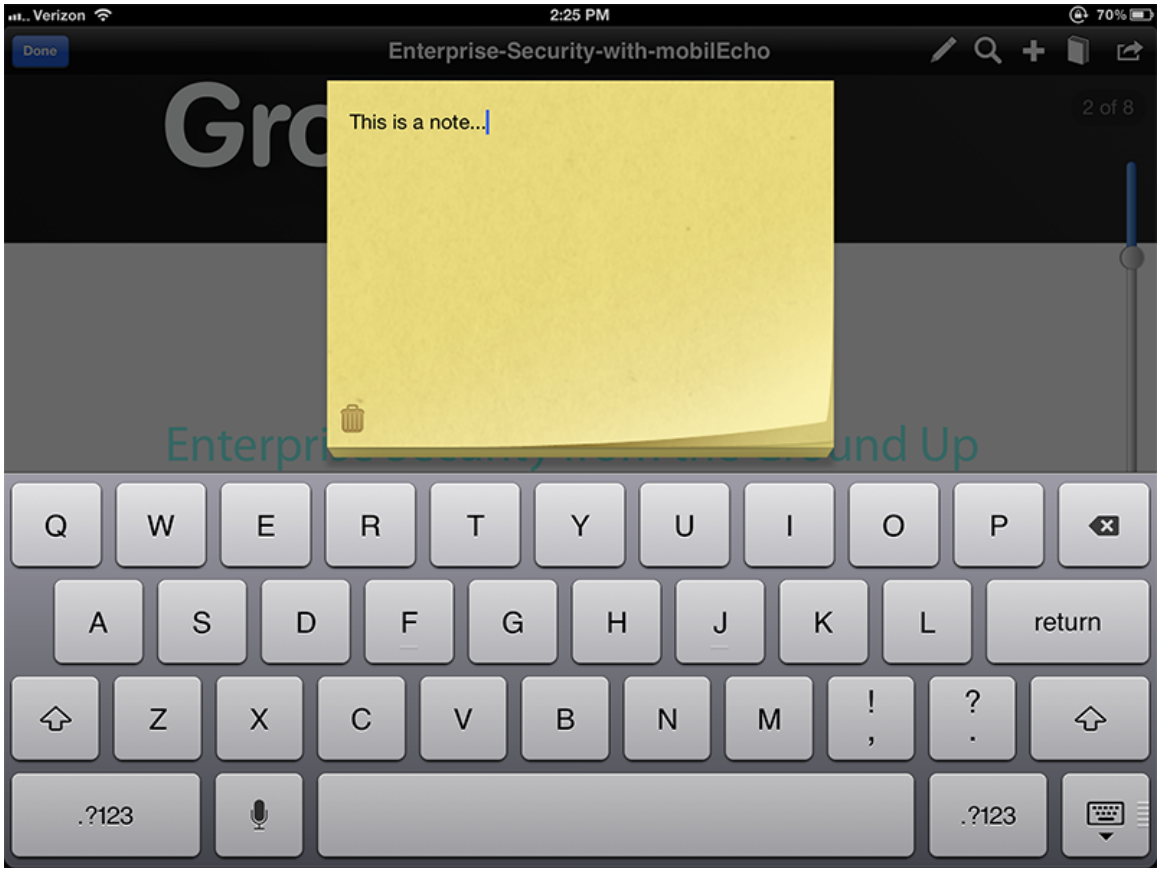
5. Once the annotation has been added, tap the annotated text again to open an options menu. This menu allows you to change parameters of the annotation, such as it's color.
6. You can also use this menu to **Clear** the annotation.



Adding a new Note, Text, Stamp, or Image to the document

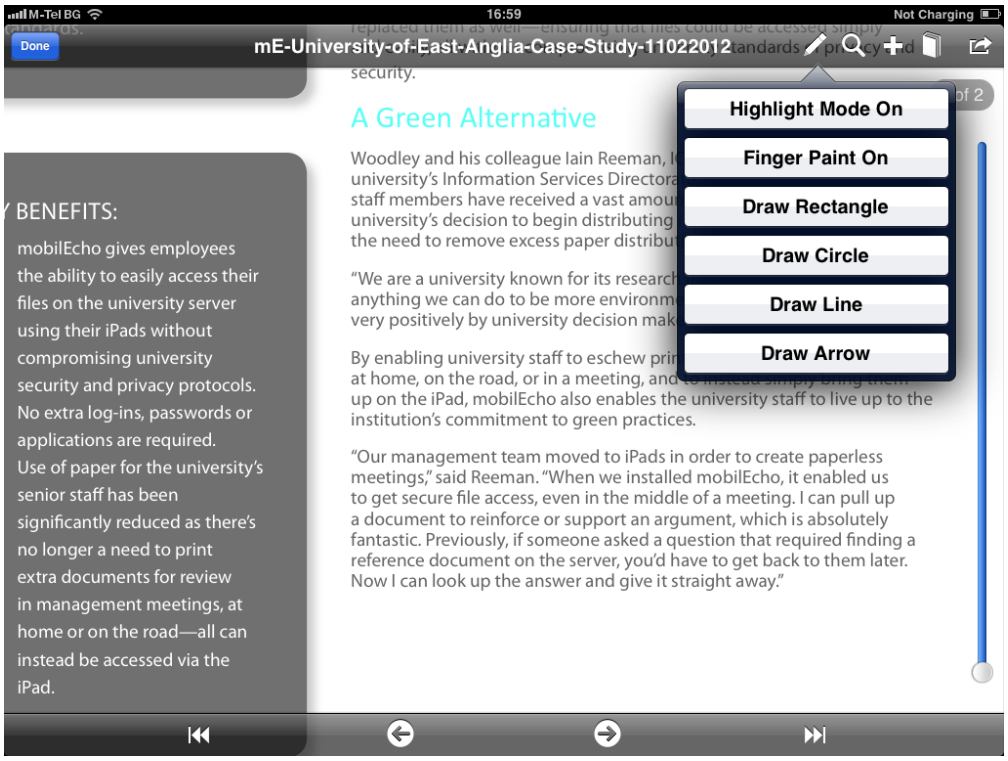
1. Tap and hold a non-text area within the document.
2. A menu will appear allowing you to select the type of annotation you would like to create.

3. For this example, we will chose **Note**.
4. An **Note** window appears. Type your **Note** text and a tap outside of the note to close it. The **Note** will appear as a **Note** icon in the document.



Adding shapes and freeform drawing

1. Tap on the **Pencil** icon in the upper right corner.



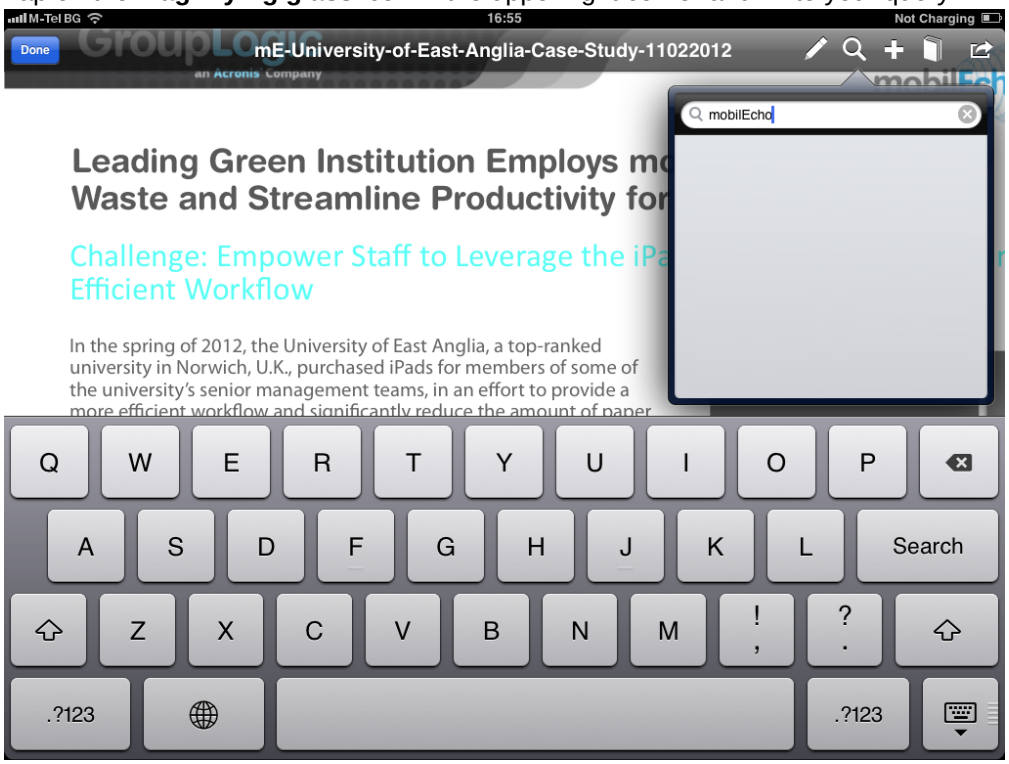
- **Highlight Mode** - starts to highlight the text from where you first tap.

- **Finger Paint** - enables touch-to-draw (freeform drawing).
- **Draw Rectangle** - places a scalable rectangle.
- **Draw Circle** - places a scalable circle.
- **Draw Line** - places a scalable line.
- **Draw Arrow** - places a scalable arrow.

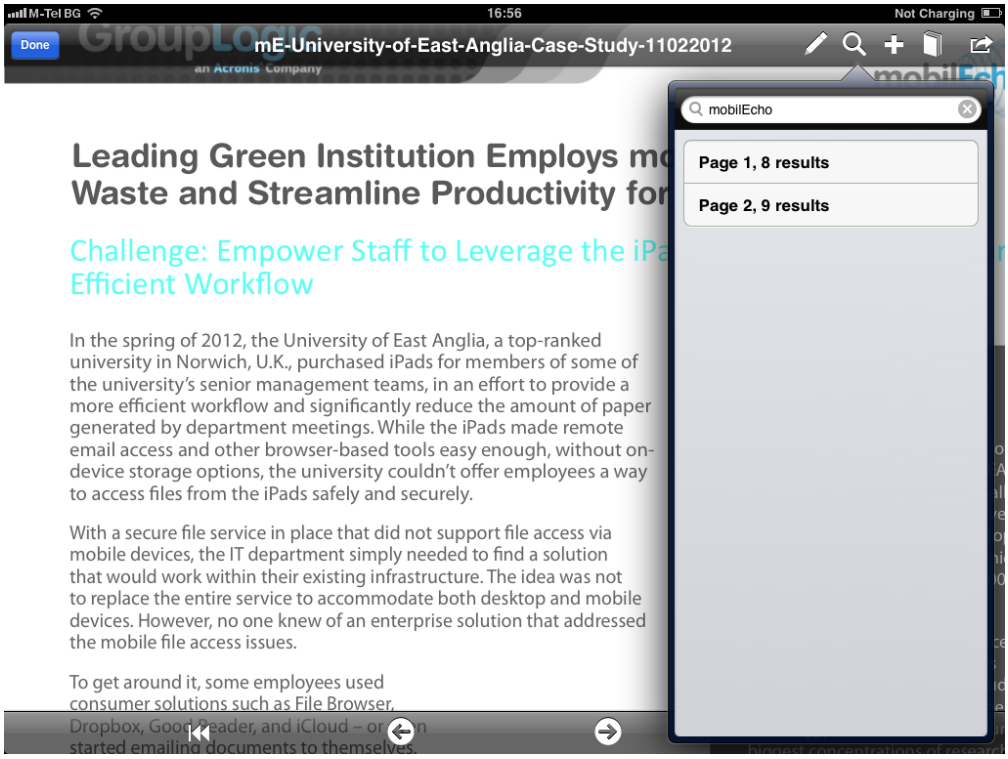
> Once the drawing/shape has been added, tap on it to open an options menu. This menu allows you to change parameters, such as the color of the drawing.

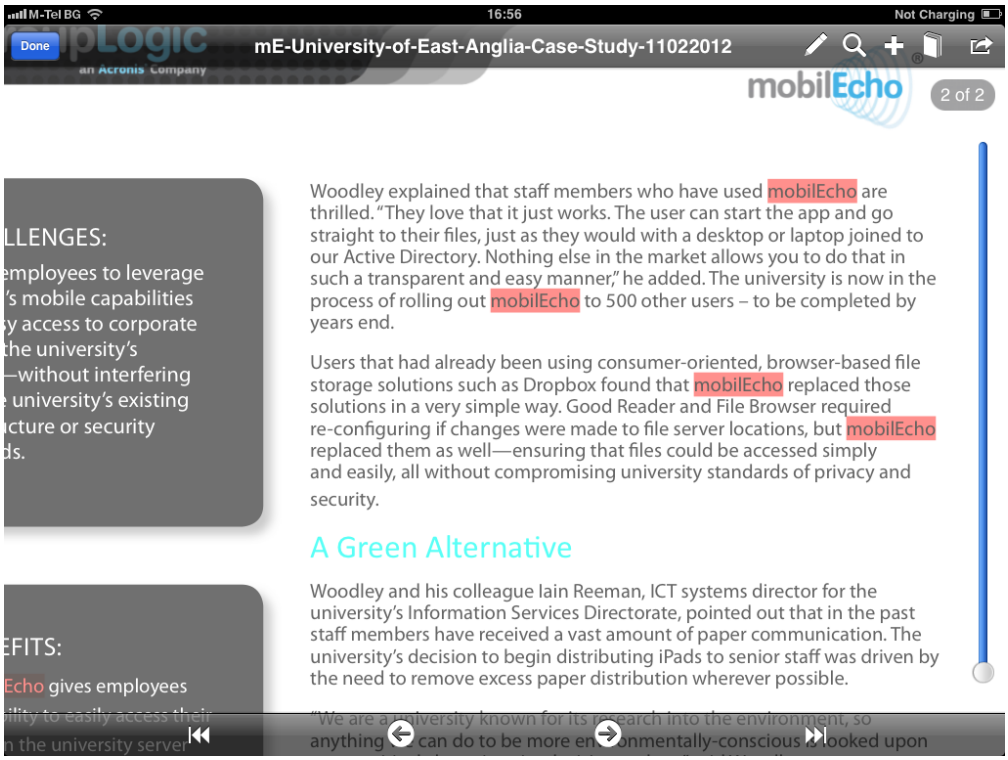
Searching a document

1. Tap on the **Magnifying glass** icon in the upper right corner and write your query.



2. Tap **Search** to get your search results (shown below). When you tap on a **search result page**, you are taken to that page and all of the found items are highlited (shown below.).

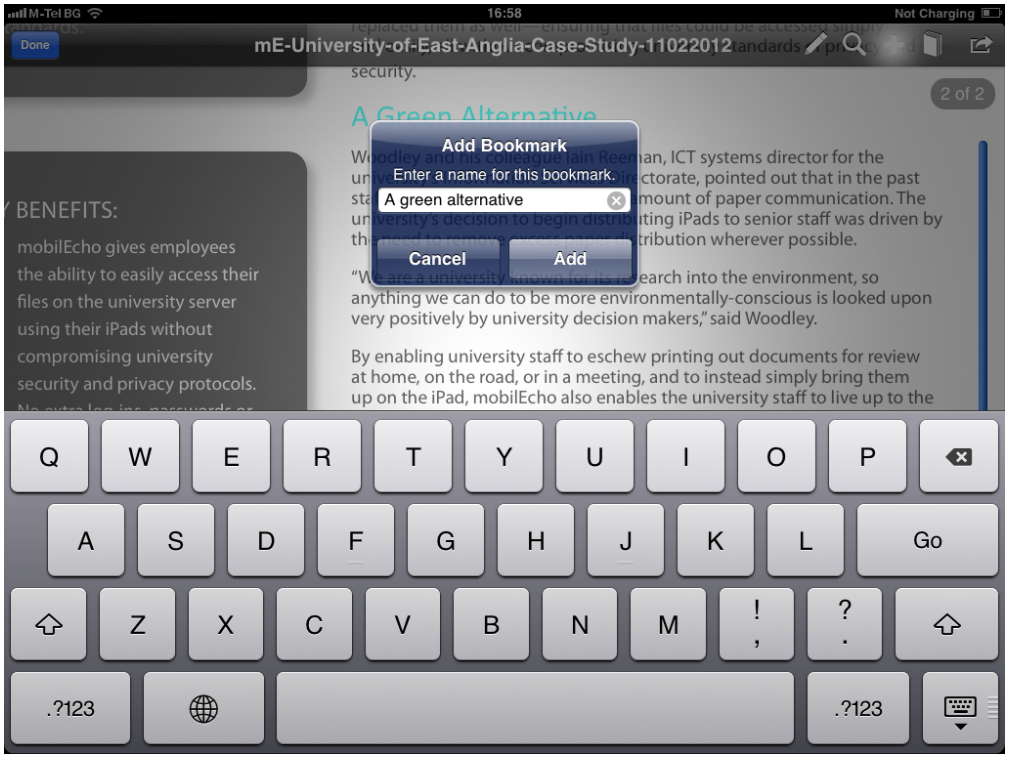




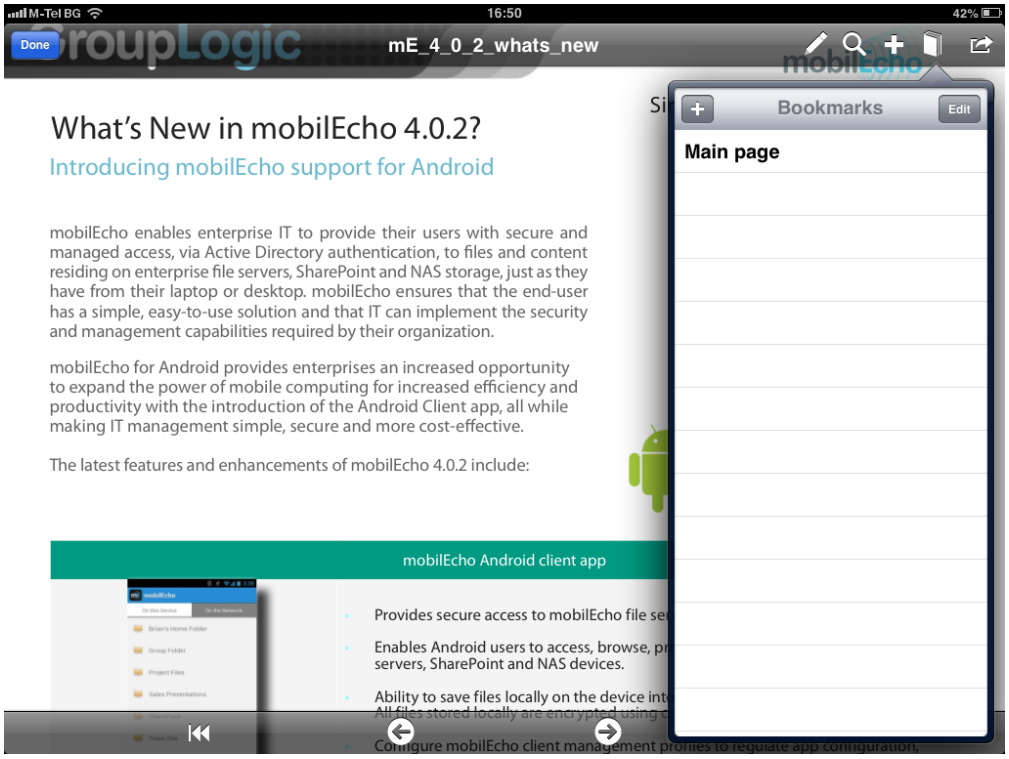
Adding a Bookmark

1. Tap on either the **Book** icon or the **Plus** icon in the upper right corner.

- If you tap on the **Plus** icon you directly start adding a new bookmark.



- If you tap on the **Book** icon, you're presented with the contents menu from which you tap on **Bookmark s** which opens the list with all existing bookmarks.



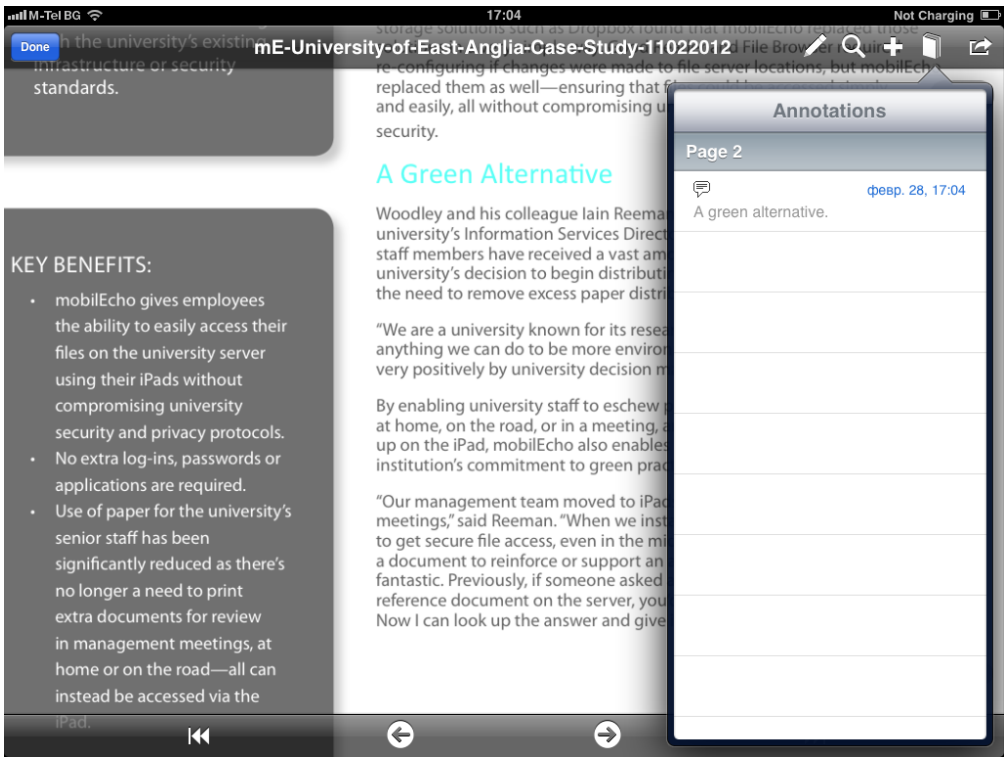
Viewing Bookmarks, Table of Contents, and the Annotations list

1. Tap on the **Book** icon in the upper right corner to open the menu.

2. From there you can open the **Bookmarks**, **Table of Contents** and **Annotations**.

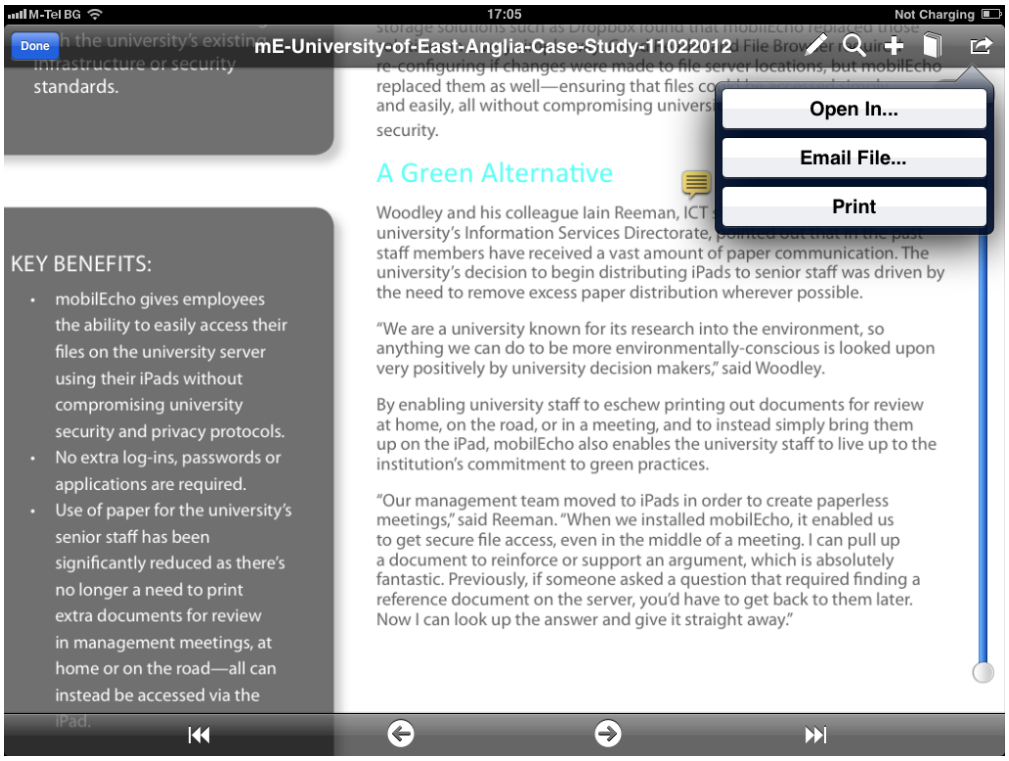
- **Bookmarks** - displays a list of the current bookmarks for this pdf.

- **Contents** - displays a list of contents for the current pdf.
- **Annotations** - displays a list of all the notes on this pdf.

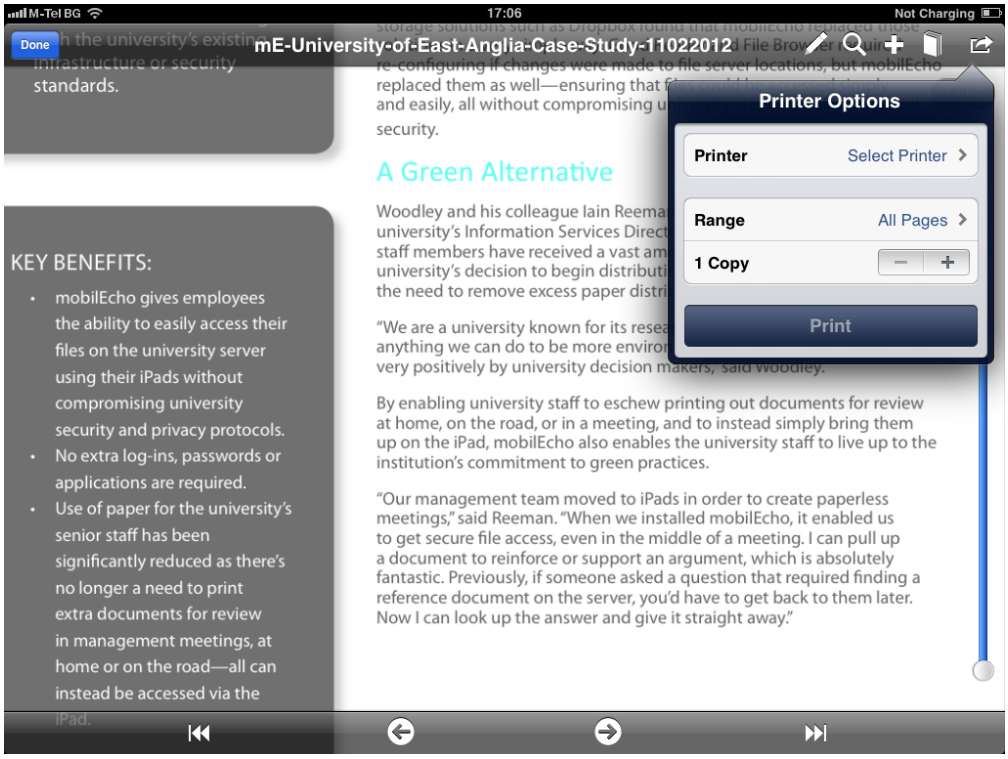


Emailing and Printing the file

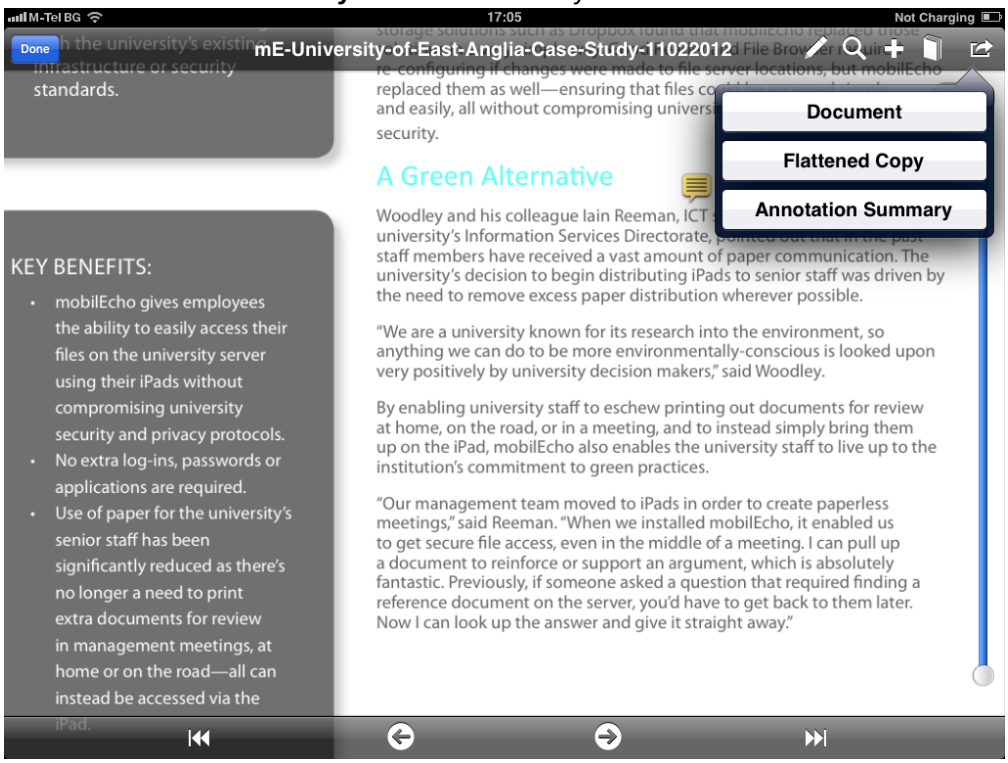
1. Tap on the **Menu** icon in the upper right corner.
2. Select either **Print** or **Email File...** .



- **Print** - opens a menu to select printer and settings before printing.

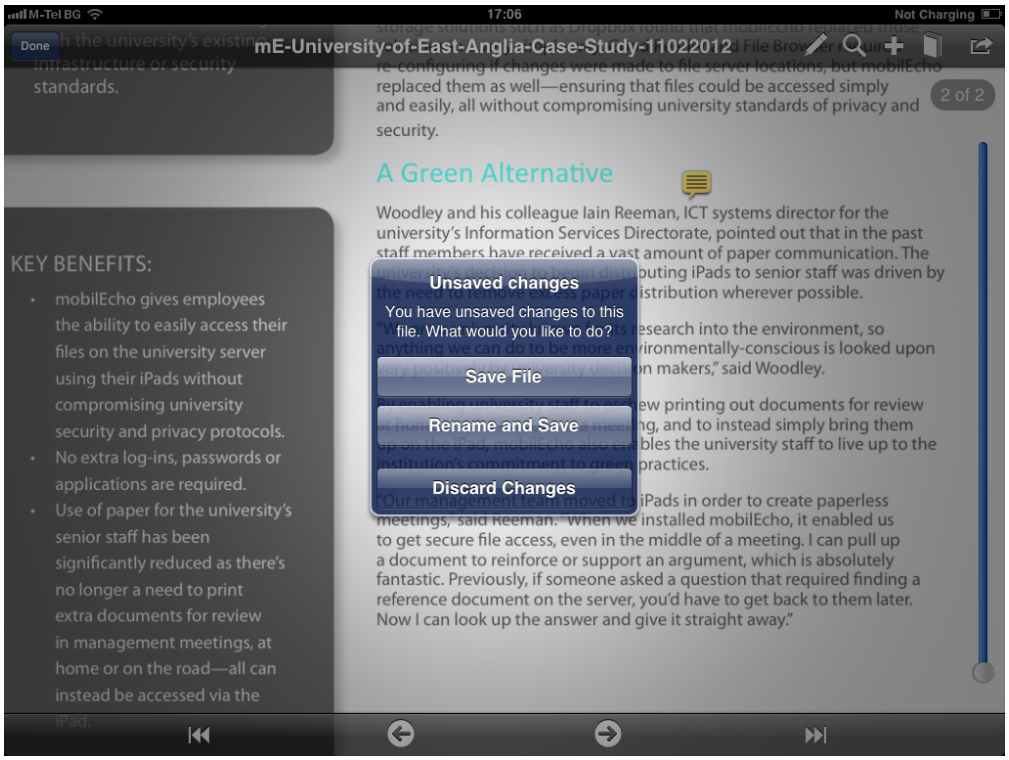


- **Email File...** - opens a menu for selecting how should the file look like before sending.
  - **Document** - sends the document.
  - **Flattened Copy** - sends a copy of the document, with all the notes saved inside it permanently.
  - **Annotation Summary** - sends a summary of the notes.



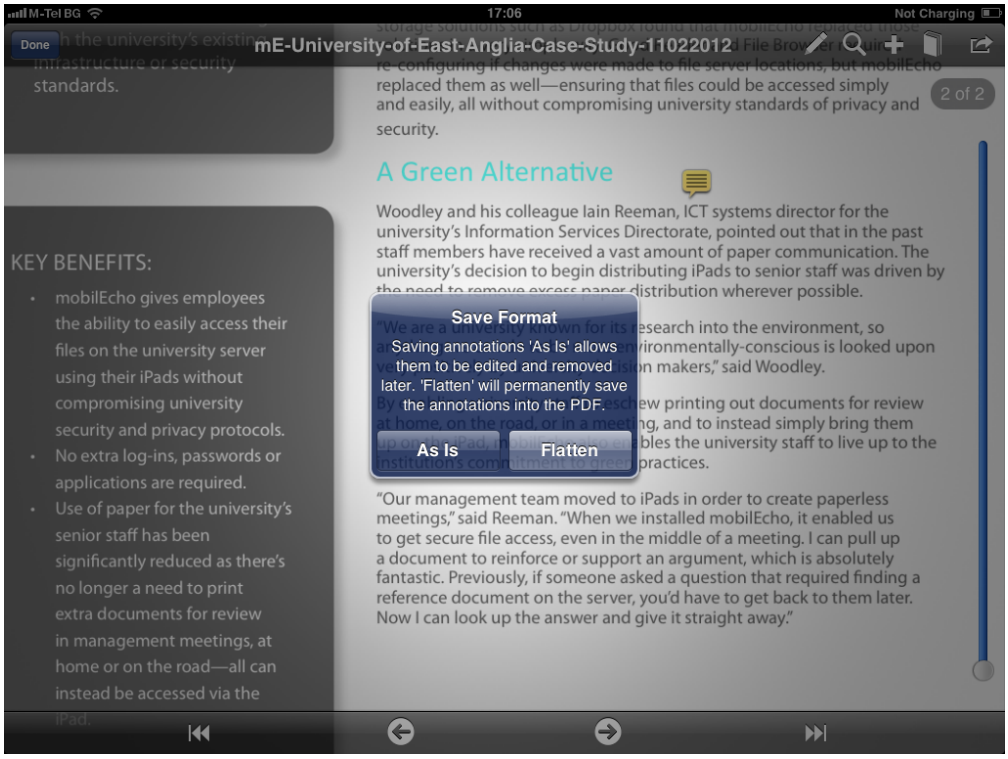
Saving an annotated file

1. Add a note to a PDF file using the mobilEcho previewer.
2. Tap **Done**.
    - **Save File** - overwrites the current file.
    - **Rename and save** - saves a renamed copy of the file.



3. Select how to save the notes.

- **As is** - saves the file with the option to edit the notes later on.
- **Flatten** - saves the file with the notes saved permanently in it.



mobilEcho Android Client Application

Installing mobilEcho for Android

mobilEcho for Android is available for free on the Google Play store. Visit the Google Play store to install mobilEcho.

Configuring mobilEcho for Android

After installing mobilEcho, you can configure it in two ways:

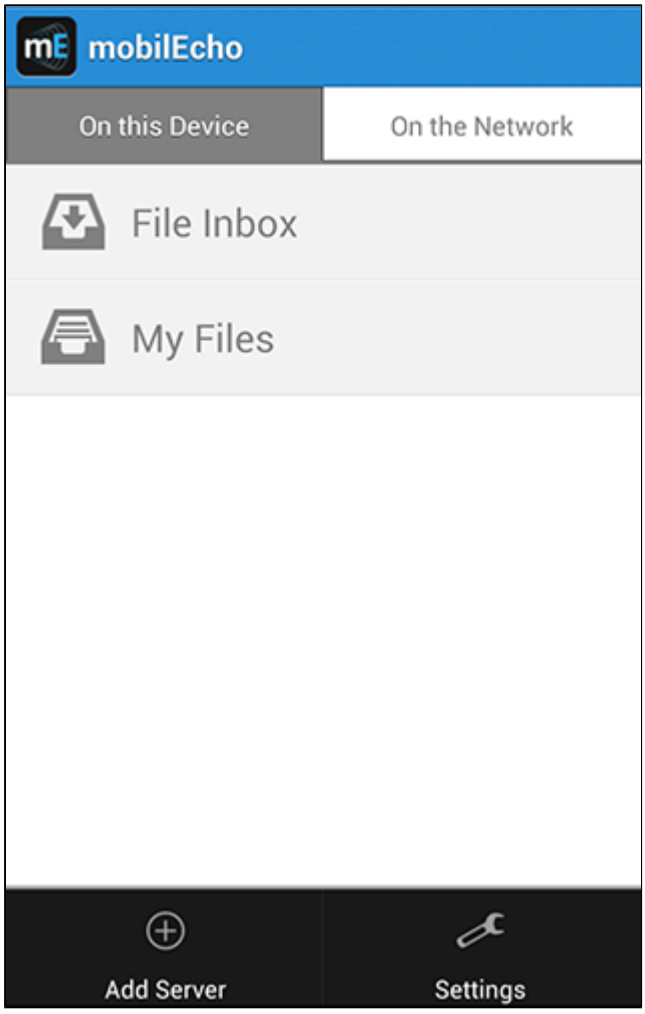
If your organization centrally manages mobilEcho access and settings, you will need to request access to mobilEcho from your IT department. You will receive an enrollment email once you've been granted access that includes the information and instructions you will need to start using mobilEcho.

If your mobilEcho server allows access without you mobilEcho client being centrally managed, you can get started by simply entering your mobilEcho servers name along with your username and

password.

To manually configure your mobilEcho server

1. Start the **mobilEcho** app. You will be taken to the mobilEcho home screen.
2. Tap the **Menu** button on your device to open the mobilEcho menu.
3. Tap the **Add Server** button.

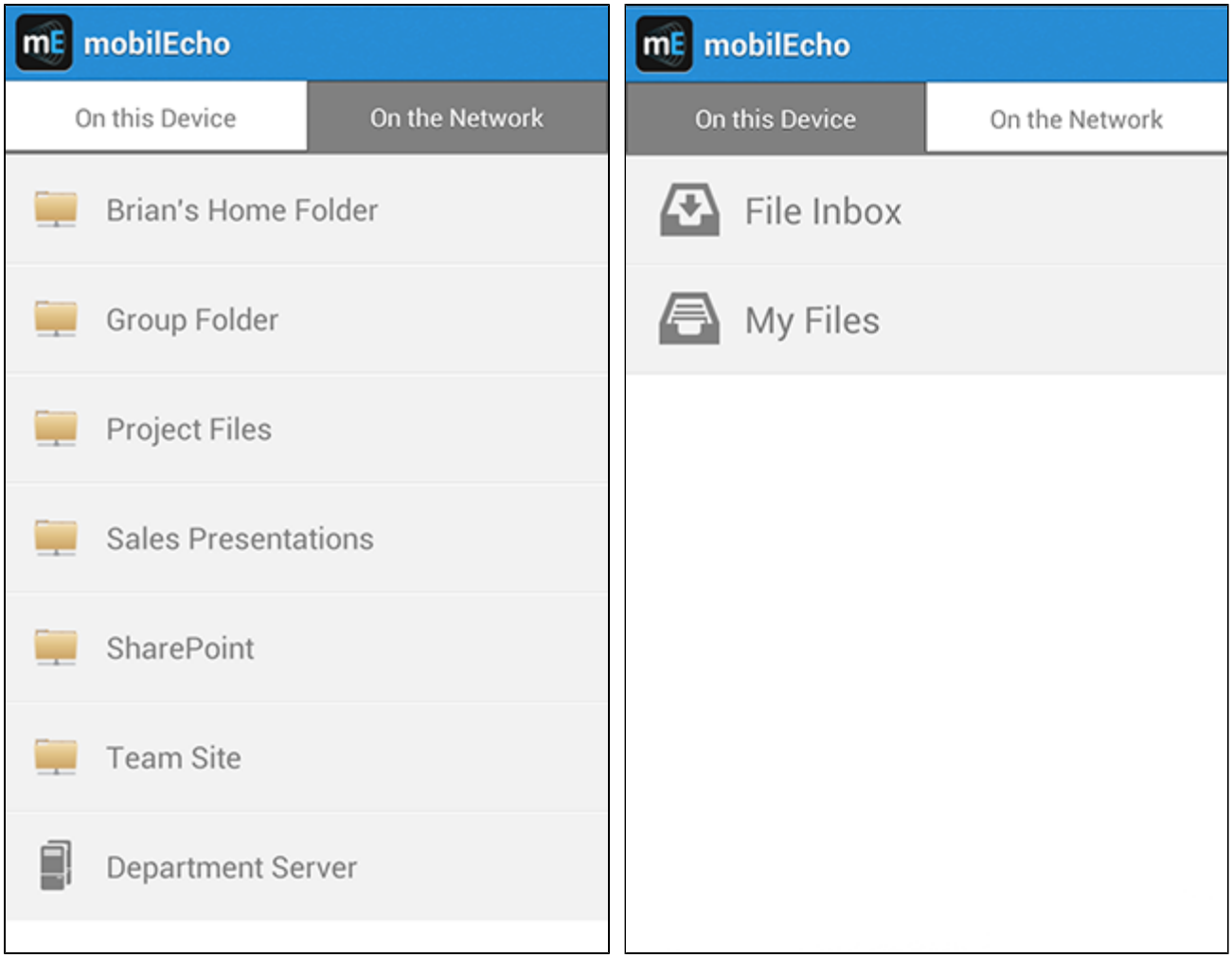


4. Enter the **server name or IP address** of your mobilEcho server. This is usually something like: **mobilecho.mycompany.com**
5. Optionally, if you would like the server to appear in the app with a name other than the **server name** you just entered, enter an alternate **Display Name** for this server.
6. Enter your **username**. This is usually the same username you use to get to other company resources and your email account.
7. If you would like to save your password, tap the **remember password** checkbox and enter and confirm your password.

8. Tap Save to finish adding this server.

Working with Files

After completing enrollment with your company's mobilEcho client management system, or after adding a server manually as detailed above, you will see one or more servers or folder in mobilEcho's **On the network** tab. Any mobilEcho files that are located within the mobilEcho app in your on-device storage are found on the **On this device** tab. Only files within the **On this device** tab will be accessible when you are not on a network that is able to connect to your company's mobilEcho server.

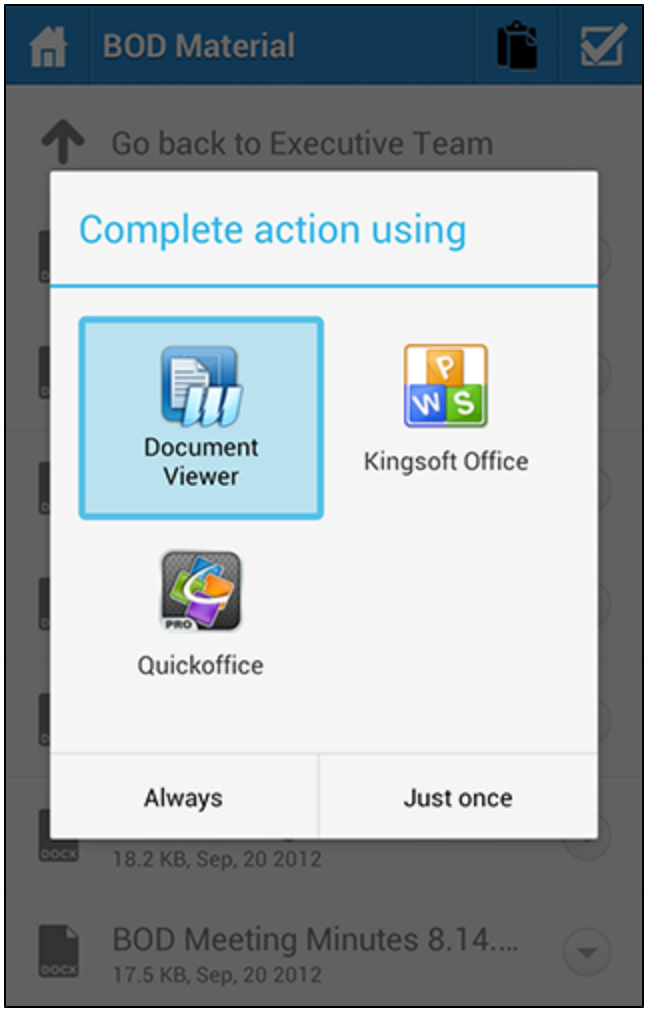


To browse files, tap on a server or folder and navigate into subfolders as needed.

Once you locate the file you're looking for, you can tap the menu button to the right side of the filename to open the file menu, or simply tap the file name itself to open the file.

Opening files into other apps on your device

When opening a file, you may be prompted to choose the application on your device that would would like to use to view or edit the file. If you choose **Always**, all file of that type will be opened into the selected app automatically in the future. If you choose **Just once**, you will be prompted to select an app again the next time you open a file of this type. This will let you work with various apps in the future, depending on what you are doing with the file. If you've chosen **Always** and would like to revert back to being able to choose from multiple apps, there is an option in your Android device's main **Settings** list that should allow you to do this.

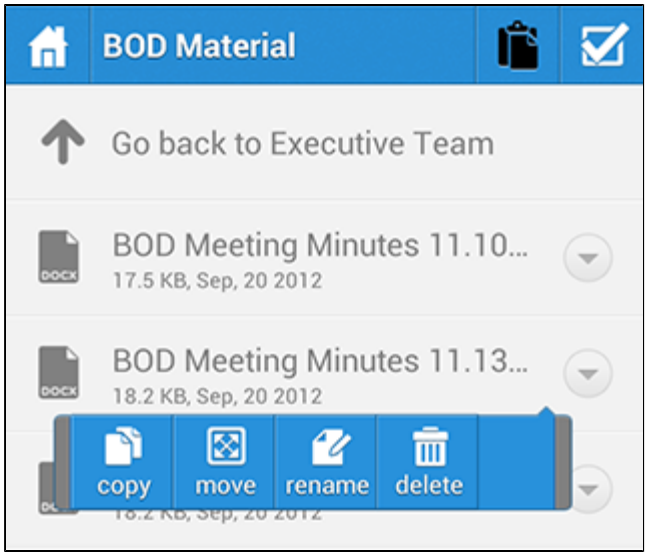


Opening files from other apps into mobilEcho

When you are working with a file in another app, you will need to use its Share or Send feature to open the file into mobilEcho when you are done. When files are sent to mobilEcho, they appear in the **File Inbox** on the **On this device** tab.

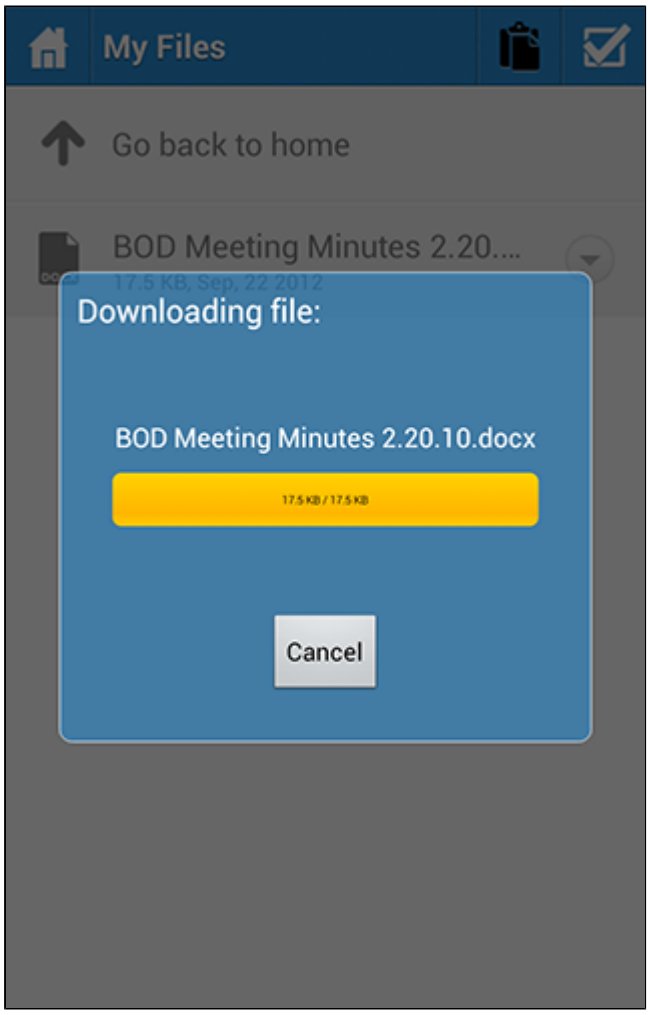
File and folder copy, move, rename and delete

1. To take action on a file or folder, tap the menu icon to the right of its name in mobilEcho.



2. Choose the desired action: **copy**, **move**, **rename**, or **delete**
3. If you are **copying** or **moving** a file, you will be prompted to navigate to the destination for the file.
4. Navigate into the folder where you would like to **copy** or **move** the file, then tap the **Clipboard** icon in the top menu bar.
5. The **Clipboard** will be displayed and include a list of the files to be copied or moved.

6. Tap the **Paste** button to copy or move the file into the current folder.



Copy, move, and delete of multiple files or folders

It is possible to copy, move, or delete more than one file at a time with mobilEcho.

To do so, tap the multi-select button  , tap the checkbox next to the files you'd like to work with, and select **Copy**, **Move**, or **Delete**.

Copying files from the server to the device for offline access

If permitted by your organization's mobilEcho client management policy, it is possible to copy files from your mobilEcho server to your device, so that you may access them even if you are not connected to a network.

To do so, use the copy instructions detailed below and copy the required files into the **My Files** folder located on the **On this device** tab.

While in the **My Files** folder, you can create new folders to organize your files by tapping your device's **M enu** button and selecting **Create Folder**.

Notes

The mobilEcho for Android app released in late September 2012 does not yet include the full set of features available in the mobilEcho for iOS app. These features will be added in followup releases. The mobilEcho features not supported on Android include:

- The app has a phone optimized UI. It will run fine on a tablet, it just won't take advantage of the extra space and present a two pane UI yet.
- PDF Annotation
- Synchronized folders
- Bookmarking of folders
- Whitelisting and blacklisting of 3rd party apps allowed to open mobilEcho files
- Filename and full content search

mobilEcho for Good Dynamics

Introduction

GroupLogic and Good Technology have partnered to bring mobilEcho's mobile file management to the Good Dynamics platform. This optional mobilEcho capability allows the mobilEcho client app to be managed, along with other Good enabled apps, using a unified set of Good Dynamics policies and services.

The components of the Good Dynamics platform include:

- **Good Control server** - A server-based console that allows the enterprise to enable client access to Good Dynamics enabled apps, create policy sets that govern application permissions and the device types they are allowed to run on, and the ability to revoke access to or wipe Good Dynamics apps on specific devices.
- **Good Proxy server** - This service is installed on an on-premise server and is used to provide network access for Good Dynamics apps needing to communicate with on-premise application servers, such as a mobilEcho file server.
- **mobilEcho for Good Dynamics app** - Good Dynamics enabled apps, such as mobilEcho for Good Dynamics, include built-in Good Dynamics services that allow the app to be remotely managed using the Good Dynamics platform and also provide the app with FIPS 140-2 certified on-device encrypted secure storage and Good secure communication.

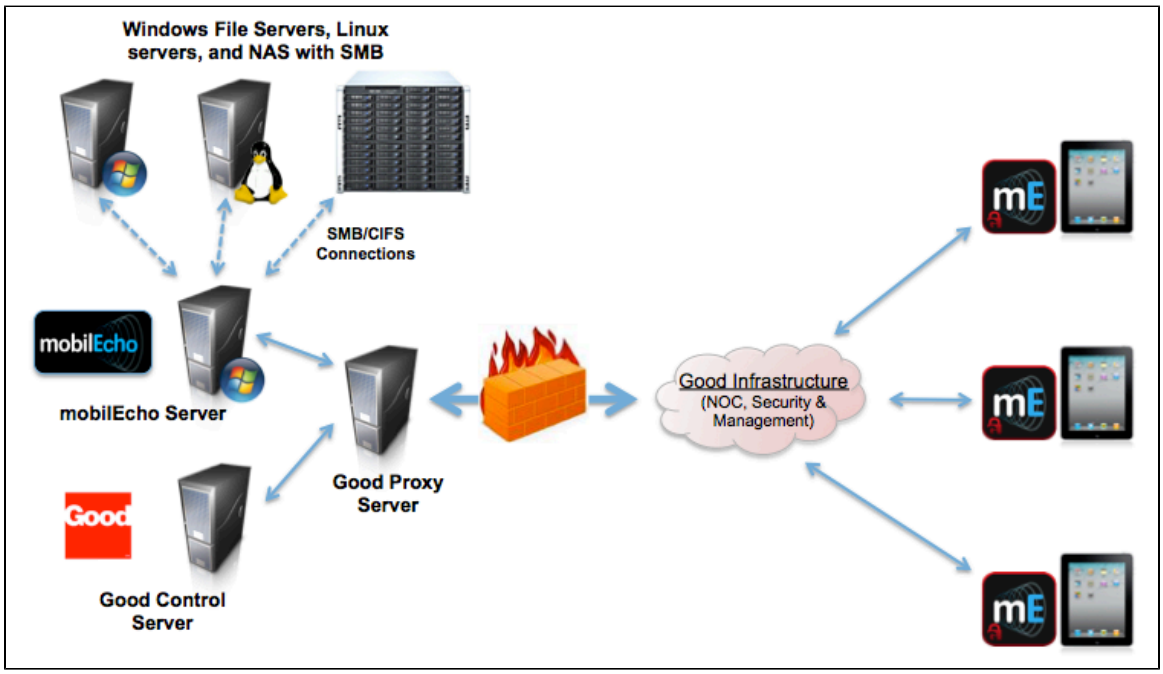
mobilEcho for Good Dynamics requires:

- **mobilEcho for Good Dynamics client app** - The mobilEcho for Good Dynamics client app available on the Apple App Store is specifically designed as a Good Dynamics integrated application. When

first installed and run on a device, the mobilEcho for Good Dynamics app will prompt the user to activate the app in Good Dynamics. This activation is required before the user can proceed with enrolling the app with their mobilEcho server and accessing file.

- **mobilEcho server** - mobilEcho for Good Dynamics uses the same server-side mobilEcho software as standard mobilEcho. No mobilEcho server-side changes are required for mobilEcho servers to work with Good Dynamics enabled mobilEcho clients. The mobilEcho server must be running mobilEcho version 3.5 or later in order for Good Dynamics enabled mobilEcho clients to be capable of saving files to the server. mobilEcho server, versions 3.7 and later, include an optional setting which allows only Good Dynamics enabled clients to connect to the mobilEcho server. This can be used to ensure that all the mobilEcho clients that have access to mobilEcho files are managed by Good Dynamics.

Once a mobilEcho for Good Dynamics client is enrolled in Good Dynamics, all communication with mobilEcho servers is routed though the Good Dynamics secure communication channel.



Testing a trial version of mobilEcho for Good Dynamics

The process of trialing mobilEcho for Good Dynamics is very much the same as a regular mobilEcho trial.

A trial version of the mobilEcho server-side software can be requested by visiting the mobilEcho Free Trial page. Once this request form has been submitted, you will receive an email with links to download the mobilEcho server trial installer and to the mobilEcho Quick Start Guide to assist in initial setup.

The mobilEcho for Good Dynamics client app is a free download from the Apple App Store.

mobilEcho for Good Dynamics client apps need to be activated in your Good Dynamics system before they can be configured for access to mobilEcho servers. When you are ready to enroll mobilEcho clients in Good Dynamics, please proceed to the following sections of this document.

Requesting and configuring mobilEcho within Good Control

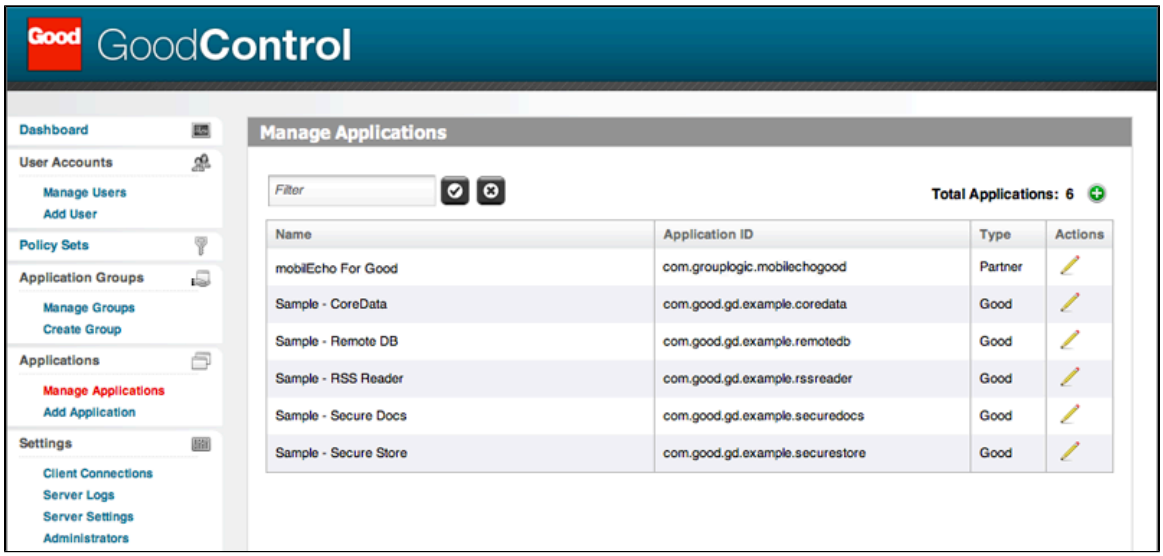
Before a mobilEcho for Good Dynamics client app can be enrolled in Good Dynamics, mobilEcho must be added to the list of **Managed Applications** on your Good Control server. For this to happen, you must

request access to the **mobilEcho for Good** app using the Good Dynamics **beGood Communities** site. If you are not currently a registered member of the beGood site, another member of your organization may be responsible for managing vendor relationships on this site, or you may simply need to register for an account with Good.

Requesting access to mobilEcho for Good Dynamics

To request to connect with GroupLogic and gain access to **mobilEcho for Good**, visit this URL: https://begood.good.com/groups/grouplogic

On the GroupLogic group page, click the **Connect** button and submit a connection request to GroupLogic. Please choose the **mobilEcho for Good** app during this process. You should receive a notification from the beGood site when your connection request has been accepted and notifying you when the **mobilEcho for Good** app as been published to your Good Control server. Once this has happened, log into your Good Control server and click Manage Applications in the lefthand menu. mobilEcho should now be listed as a Partner app in your managed applications list.

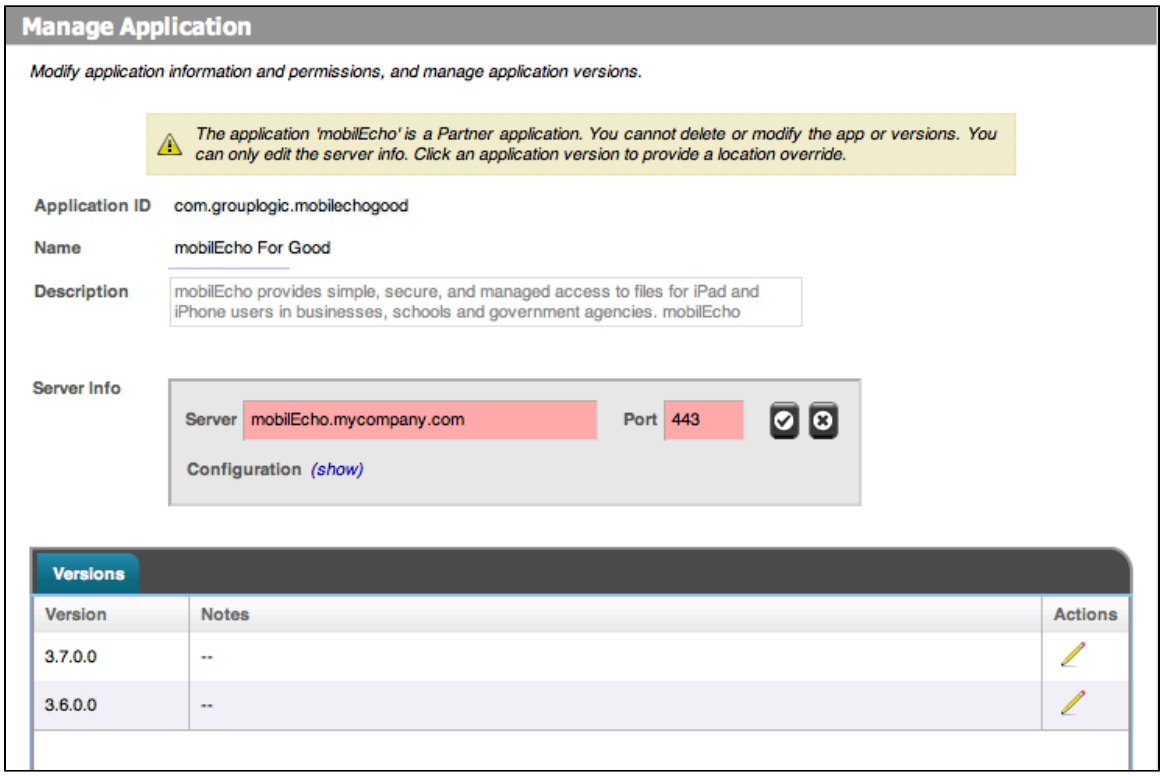


Configuring Good Proxy access to your mobilEcho server(s)

In order for mobilEcho clients to be able to access your mobilEcho server through the Good Proxy server, you will need to enter the address of your mobilEcho server in the application's configuration. If you have more than one mobilEcho server, configure access to one mobilEcho server here and additional servers can be added on the Client Connections page in the Good Control console. Details on doing so are included below.

Click the **mobilEcho** app in the **Manage Applications** list to open its settings.

In the **Server Info** box, enter the DNS name or IP address of your mobilEcho server. The **Port** number is usually **443**, unless you've configured mobilEcho to run on a non-standard port. All communication between mobilEcho clients and mobilEcho servers occurs on port 443 by default. Click the 'Check' button to save this change.

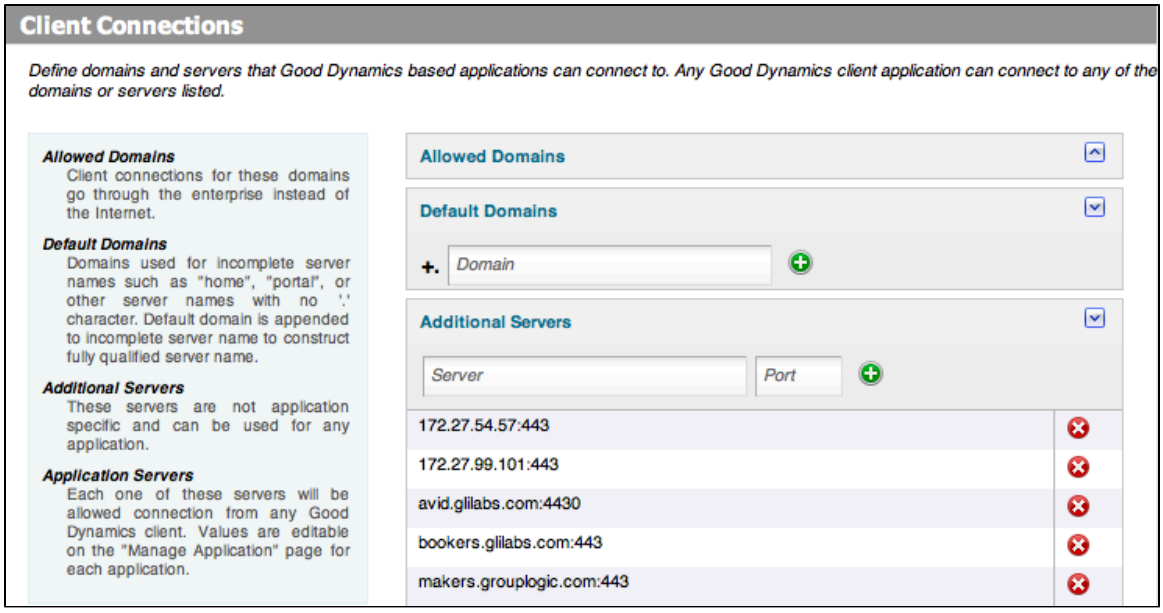


Allowing access to multiple mobilEcho servers

If you have more than one mobilEcho server on your network, you will have to allow additional server addresses in the Good Control console. If you do not so this, mobilEcho client will only be able to connect to the single server you configured in the previous step.

To permit acces to additional mobilEcho servers, select the **Client Connections** item in the lefthand menu in the Good Control console.

In the **Additional Servers** box, enter the mobilEcho server's DNS name or IP address and it's port, then click the "+" icon to add it to the list. The default mobilEcho server port is 443.



Good Dynamics Policy Sets and mobilEcho

The mobilEcho for Good Dynamics app respects the policy settings included in a user's assigned **Policy Set**. Policy sets are configured on the Good Control server.

These settings include:

- Application lock password requirements
- Lock screen policies
- Data leakage protection
- Permitted iOS versions and hardware models
- Connectivity verification
- Jailbreak/root detection

Data Leakage Protection effects and limitations

NOTE: If **Data Leakage Protection** is enabled in a policy set, the mobilEcho client app will not be permitted to:

- Open files into standard 3rd party applications on the device
- Receive files from other standard 3rd party applications on the device
- Email files using the iOS email client
- Print files
- Copy and paste text from within previewed files

If you require these features, you will need to enable the **"Disable Data Leakage Protection"** check box in the applicable Good Policy Set.

mobilEcho for Good Dynamics includes a Good Dynamics feature called "Secure Docs". This allows files to be transferred between the mobilEcho for Good Dynamics app and the Good for Enterprise app. Once a file is opened into the Good for Enterprise app, it can then be opened into other 3rd party Good Dynamics enabled apps that include this feature. This functionality is be available, even with the Good Control **Data Leakage Protection** policy setting enabled.

An upcoming version of mobilEcho for Good Dynamics will add the ability to transfer files directly between the mobilEcho for Good Dynamics app and other 3rd party Good Dynamics apps. This capability requires changes to mobilEcho for Good Dynamics and to the 3rd party apps involved, so any app that you need to transfer files to will also need to be updated by its vendor.

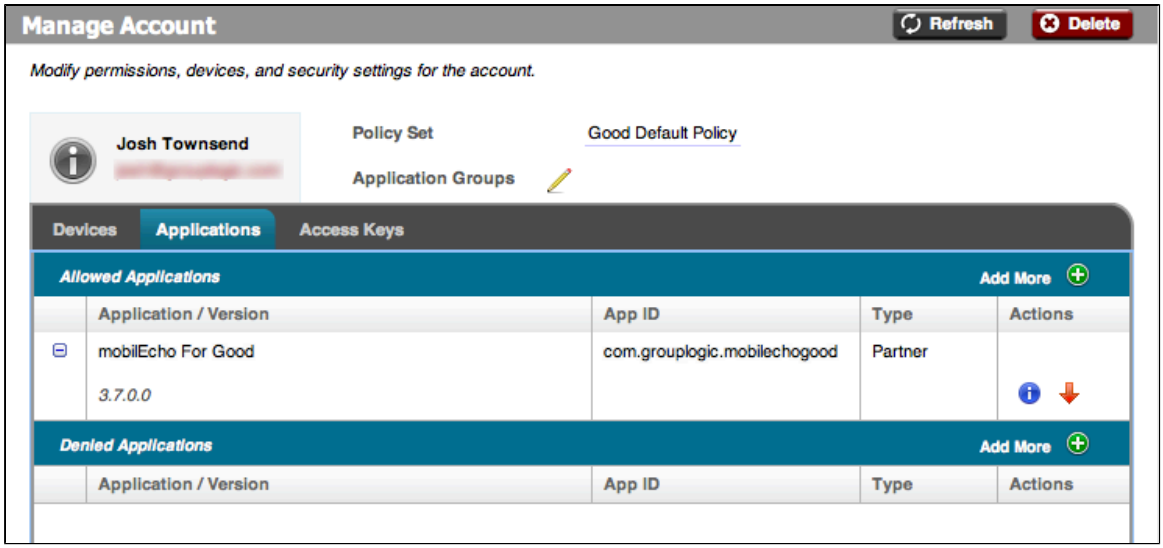
Granting mobilEcho access to a Good Dynamics User or Group

Before a user can enroll their mobilEcho client app in Good Dynamics, they must have the mobilEcho application added to their user accounts **Allowed Applications** list or to an allowed **Application Group** t hey belong to. In addition, a unique **Access Key** must be sent to the user and entered into the mobilEcho app during the enrollment process.

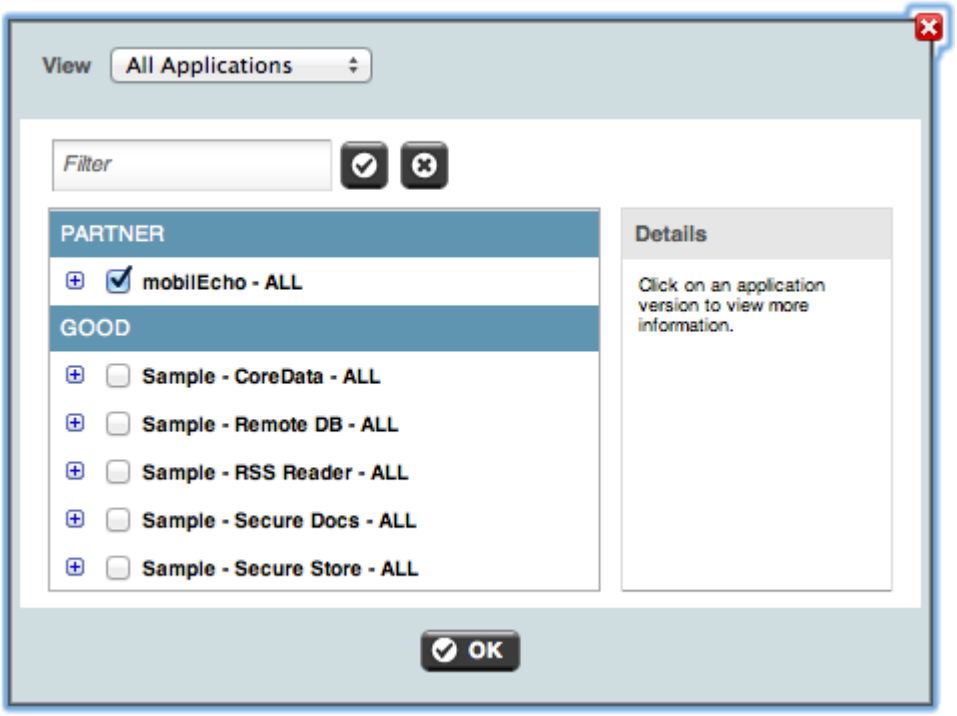
IMPORTANT DEPLOYMENT NOTE: When you assign access to Good Dynamics applications to individual users, you are required to select specific version numbers of the app to allow. If you managed access on the user level, when new versions of mobilEcho for Good are released, you will need to return to the users' Good Control configuration and add the new version before they are allowed to run that version. We **highly recommend** that you allow access to Good Dynamics apps using the **Manage Groups** functionality in the Good Control console. Good Control allows you to give a group access to ALL versions of an app, so that future versions will be allowed without IT admin intervention.

To add the mobilEcho app to an **Allowed Applications** list in a **User Account** or **Application Group**:

1. Select **Manage Groups** or **Manage Users** from the lefthand menu in the Good Control console.
2. Select the group or user you'd like to give access to mobilEcho for Good.
3. On the **Applications** tab, click the **Allowed Applications** "**Add More**" button.

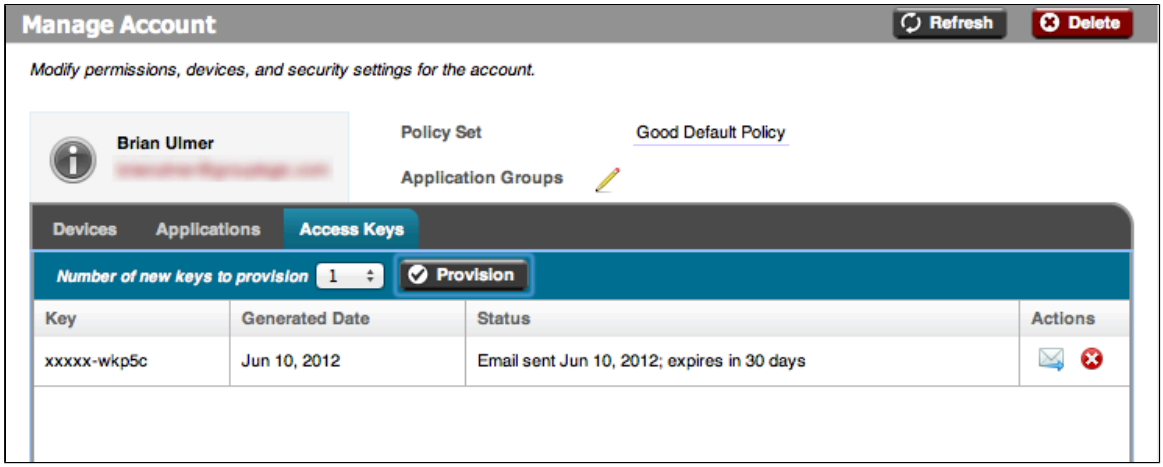


4. Select **mobilEcho for Good** from the list of available applications and click **OK**.



To generate an **Access Key** that will allow a user to enroll their mobilEcho for Good app with Good Dynamics:

1. Select **Manage Users** from the lefthand menu in the Good Control console.
2. Select the user you'd like to create an **Access Key** for.
3. On the **Access Keys** tab, select the number of keys you'd like to send and click the **Provision** button.



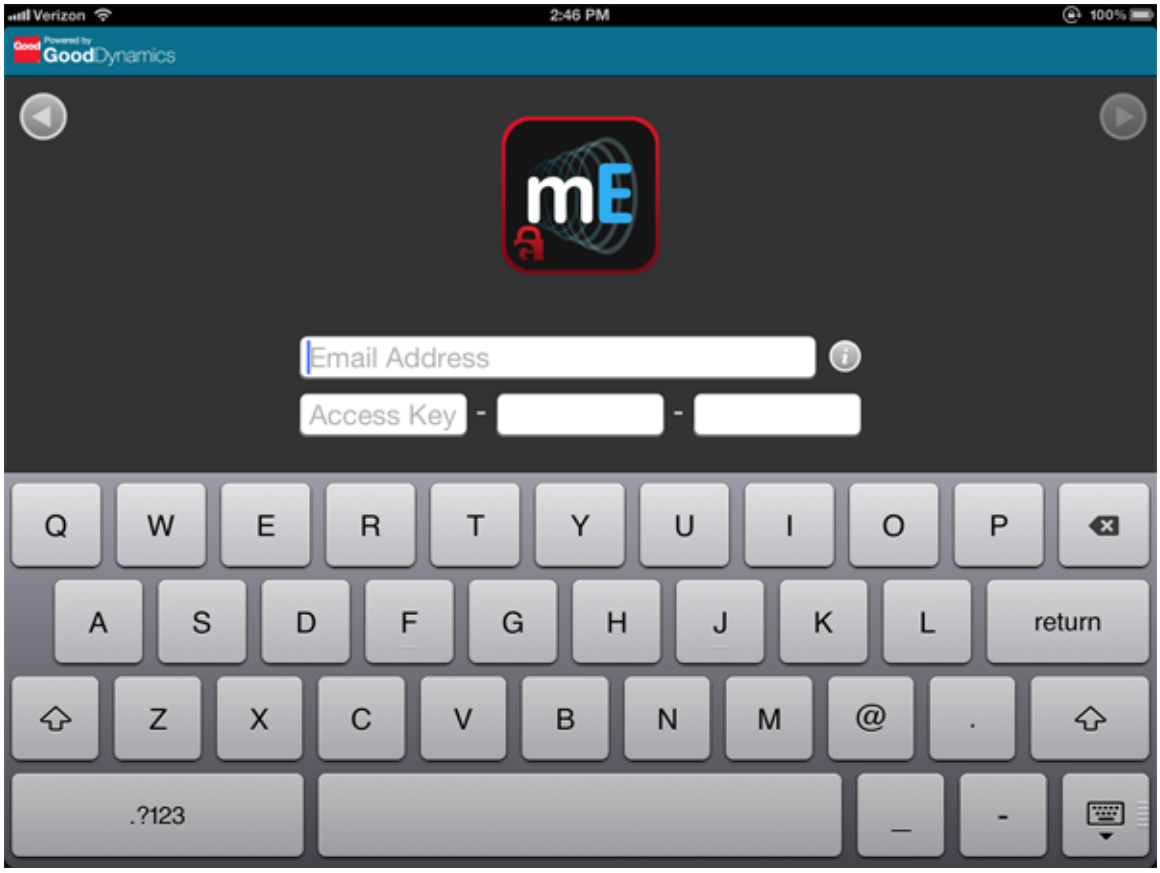
The user will receive an email that includes the **Access Key** and some basic Good Dynamics instructions.

Enrolling the mobilEcho client app in Good Dynamics

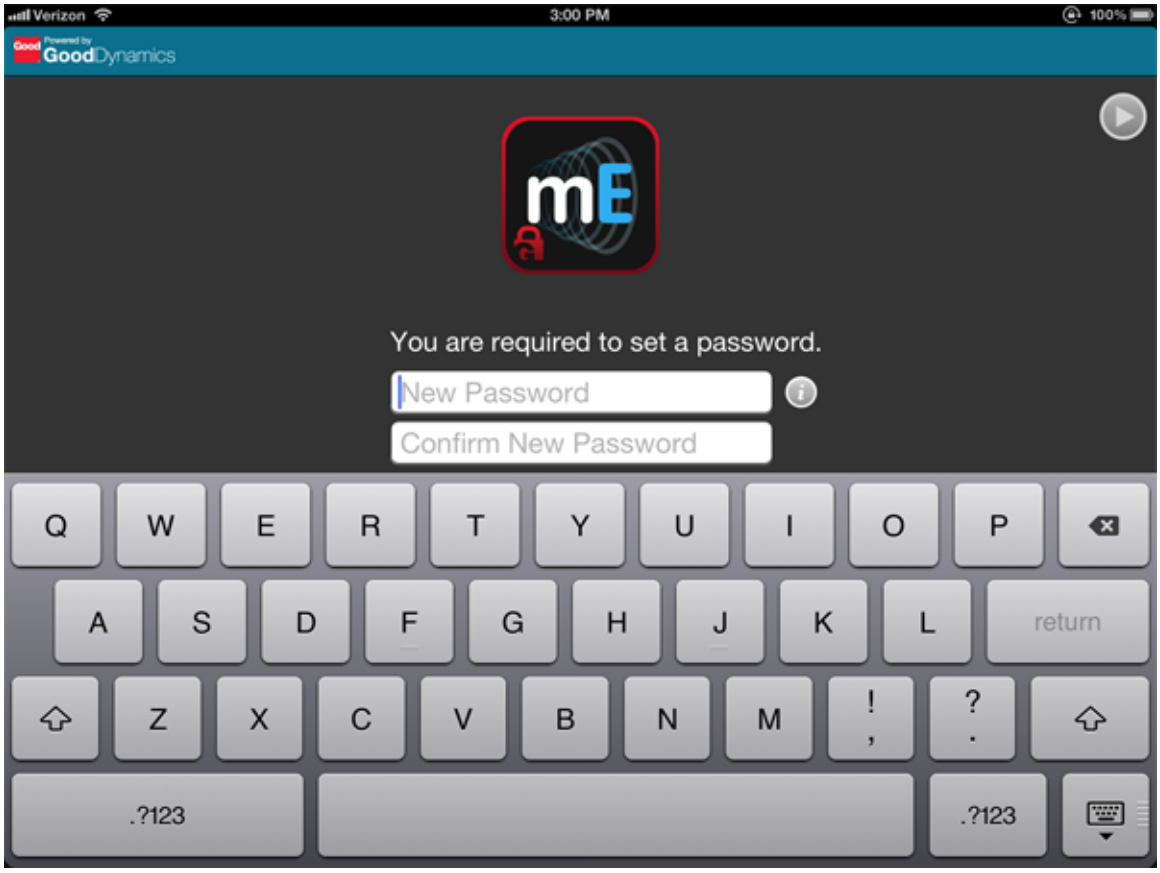
The mobilEcho for Good client app available on the Apple App Store is purpose build as a Good Dynamics integrated application. When first installed on a device, the mobilEcho app starts and required the user to activate it in your Good Dynamics system.

To enroll a mobilEcho client app in Good Dynamics:

1. Launch **mobilEcho for Good Dynamics** on your device.
2. Enter your **Email Address** and the **Access Key** that was emailed to you by your IT administrator.

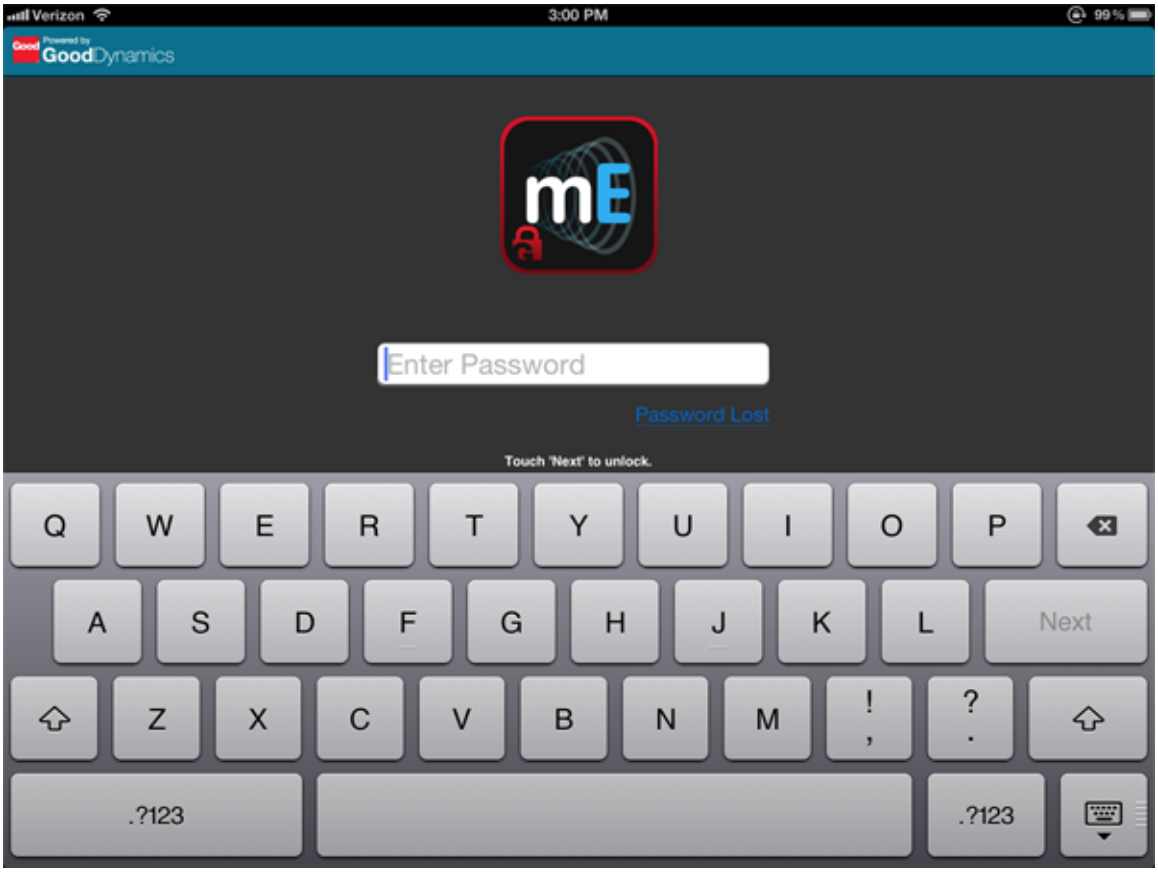


3. Progress will be displayed as your app is enrolled with Good Dynamics.
4. If required by your Good Dynamics policy, you will be asked to set an application lock password. If you are also using Good for Enterprise, mobilEcho may require that you log into Good for Enterprise in order to gain access to the mobilEcho app.



5. Once this process is completed, you will be taken to the mobilEcho application's home screen.

From this point on, when you start the mobilEcho app, you may be required to enter the mobilEcho for Good Dynamics application password that you configured earlier, or you may be required to authenticate with your Good for Enterprise app before mobilEcho opens.



Aside from that requirement, mobilEcho for Good Dynamics functions the same way that standard mobilEcho does. Some features in the app may be restricted based on your Good Dynamics policy set. This includes features such as opening mobilEcho files into other 3rd party applications, emailing and printing files, copying and pasting text from mobilEcho file previews, etc.

Once the mobilEcho for Good Dynamics app has been activated in Good Dynamics, it is not possible to deactivate. If you need to switch to a standard version of mobilEcho, you will need to delete the mobilEcho for Good Dynamics app and reinstall the standard mobilEcho app by visiting the Apple App Store.

How to use mobilEcho with Microsoft Forefront Threat Management Gateway (TMG)

Introduction

mobilEcho's iPad clients connect to the mobilEcho server running inside your firewall securely via HTTPS and need to traverse your firewall via either VPN, HTTP reverse proxy or an open HTTPS port. This article provides step by step instructions that enable connections by your user running mobilEcho client from outside your network using the "reverse proxy" functions of the Microsoft Forefront Threat Management Gateway (TMG) software, which is the successor to ISA Server 2006.

Forefront Threat Management Gateway (TMG) is a secure web gateway that enables safe employee web use through comprehensive protection against malware, malicious web sites and vulnerabilities. Building on its predecessor, ISA Server 2006, TMG provides new URL filtering, anti-malware, and intrusion-prevention technologies to protect businesses against the latest web-based threats. These technologies are integrated with core network protection features such as firewall and VPN to create a unified, easy-to-manage gateway.

The Forefront TMG solution includes two separately licensed components:

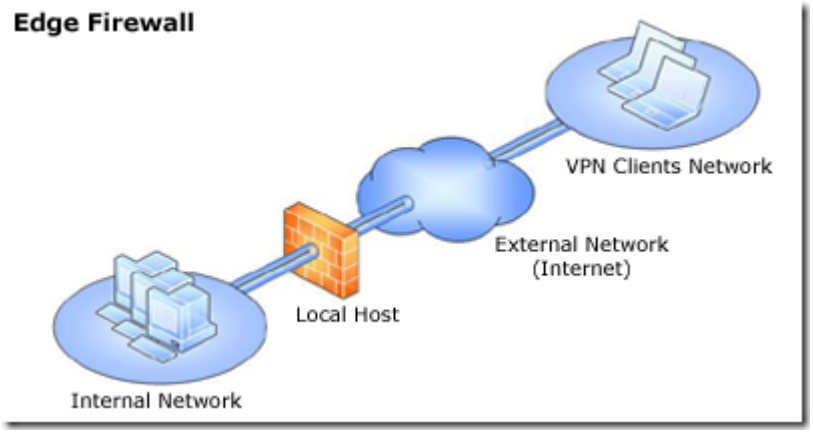
• Forefront TMG server that provides URL filtering, antimalware inspection, intrusion prevention, application- and network-layer firewall and HTTP/HTTPS inspection in a single solution.

• Forefront TMG Web Protection Service that provides the continuous updates for malware filtering and access to cloud-based URL filtering technologies aggregated from multiple Web security vendors to protect against the latest Web-based threats.

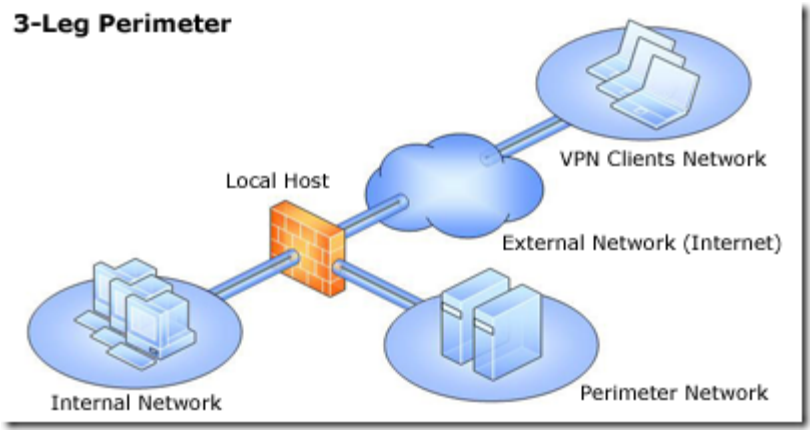
Understanding Forefront Threat Management Gateway (TMG) Network Topology

Forefront TMG includes four different network templates, that can fit in your existing network topology. It is important to choose the most appropriate for your organization option. After installing TMG, the **Getting Started Wizard** will appear, where you need to make initial configuration to your TMG. The first menu of the **Getting Started Wizard** is **Configure Network Setting**, where you need to make your choice about what network template to use. See bellow the available options.

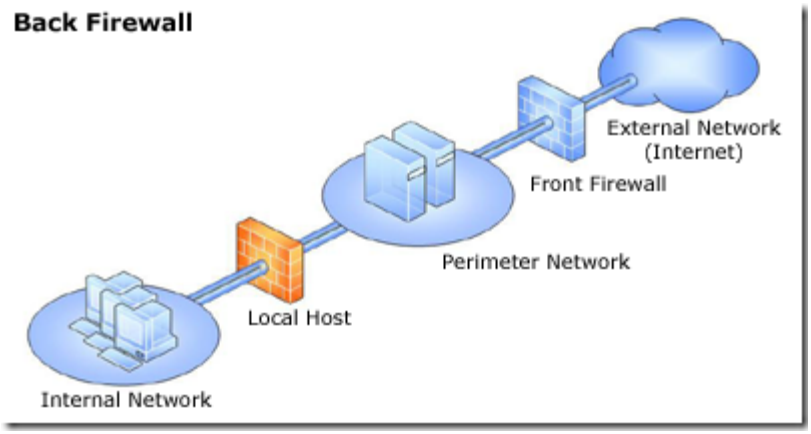
- **Edge Firewall** - In this topology, Forefront TMG is located at the network edge, where it serves as the organization's edge firewall, and is connected to two networks: the internal network and the external network (usually the Internet).

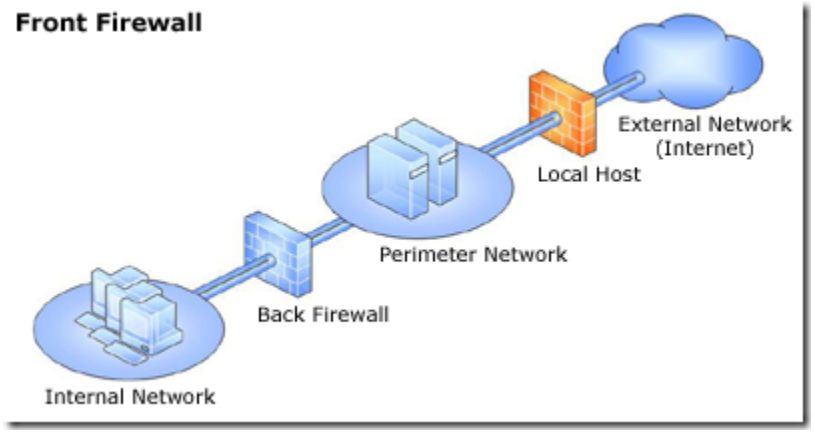


- **3-Leg Perimeter** - This topology implements a perimeter (DMZ) network. Forefront TMG is connected to at least three physical networks: the internal network, one or more perimeter networks and the external network.

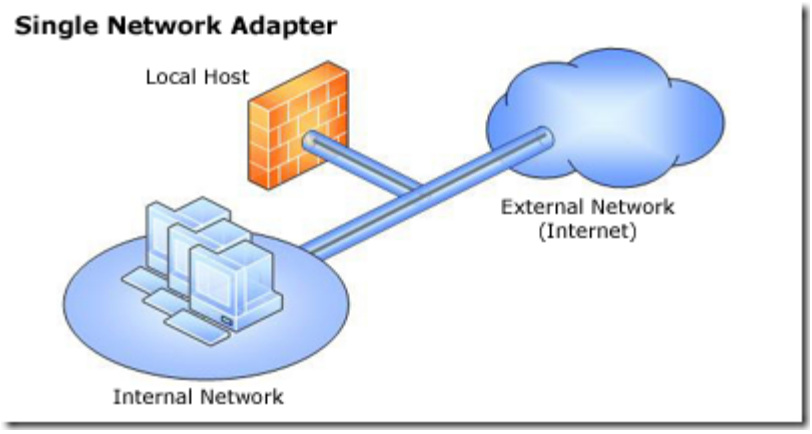


- **Back/Front Firewall** - In this topology, Forefront TMG is located at the network's back-end. Use this topology when another network element, such as a perimeter network or an edge security device, is located between Forefront TMG and the external network. Forefront TMG is connected to the internal network and to the network element in front of it.





- **Single Network Adapter** - This topology enables limited Forefront TMG functionality. In this topology, Forefront TMG is connected to one network only, either the internal network or a perimeter network. Typically, you would use this configuration when Forefront TMG is located in the internal corporate network or in a perimeter network, and another firewall is located at the edge, protecting corporate resources from the Internet.



INFO

- For more information about how to install and configure TMG visit: http://technet.microsoft.com/en-us/library/cc441445.aspx.
- For TMG minimum systems requirements visit: http://www.microsoft.com/forefront/threat-management-gateway/en/us/system-requirements.aspx.
- For pricing details visit: http://www.microsoft.com/forefront/threat-management-gateway/en/us/pricing-licensing.aspx.

Go to top

Understanding Forefront Threat Management Gateway authentication

TMG provides 3 general methods of authenticating users and they are:

HTTP authentication:

- Basic authentication - The user enters a username and password which the TMG server validates against the specified authentication server.
- Digest and WDigest authentication - Has the same features as the Basic authentication but provides a more secure way of transmitting the authentication credentials.
- Integrated windows authentication - Uses the NTLM, Kerberos, and Negotiate authentication mechanisms. These are more secure forms of authentication because the user name and password are hashed before being sent across the network.

Forms-based authentication:

- Password form - Prompts the user to enter a username and a password.
- Passcode form - Prompts the user to enter a username and a passcode.
- Passcode and Password form - Prompts the user to enter a username/password combination and a username/passcode combination.

Client certificate authentication

When users make a request for published resources, the client certificate sent to Forefront TMG is passed to a domain controller, which determines the mapping between certificates and accounts. The certificate must be matched to a user account.

> **Note:**
>
> Client certificate authentication is not supported for authenticating outbound Web requests.

> **INFO**
>
> For more information on TMG authentication, please visit these sites:
> http://technet.microsoft.com/en-us/library/cc441695.aspx
>
> http://technet.microsoft.com/en-us/library/cc441713.aspx

Go to top

Overview

> **INFO**
>
> This document covers the case when TMG is used as an Edge Firewall. If your organization uses TMG in a different network topology please contact GroupLogic for specific instructions.

If you are using Microsoft Forefront Threat Management Gateway (TMG) to dedicate and protect your internal network from Internet threats and viruses, you need to make certain configurations to your TMG server to get it working with mobilEcho. To use TMG as reverse proxy and firewall for your mobilEcho server you need to create two separate networks on your TMG computer: internal and external. The two TMG network adapters should be properly configured, one with a private (internal IP address) and one with a public (external IP address). The mobilEcho server should be part of the internal network.

To use mobilEcho with TMG you need to complete the steps described in this document:

- Obtain a SSL server certificate and install it to your mobilEcho server and to the TMG server computer.
- Create a web listener in TMG.
- Create new web site publishing rule for the mobilEcho file server, so that the clients from outside your network can connect to mobilEcho.
- Create an external DNS record in your DNS server.

The mobilEcho client app supports these forms of authentication with a reverse proxy server:

- Pass-through authentication
- HTTP authentication (username & password)
- Certificate authentication

Go to top

Install the SSL Server Certificate

Request and install a SSL certificate using the FQDN for each mobilEcho file server you want to publish via TMG in order to prevent DNS spoofing. You need to install the root SSL certificates on the TMG computer. These certificates should match the FQDN of each published server.

Follow the steps bellow to import a certificate to the TMG computer:

1. On the TMG computer, click **Start**, type **mmc**, and then press **Enter** or click **OK**.
2. Click the **File** menu and then click **Add/Remove Snap-in** or press **Ctrl+M**. Under **Available Snap-ins**, click **Certificates** and then click **Add**.
3. Select Computer Account and then click **Next**, click **Local Computer** and then click **Finish**.
4. Click **OK** in the **Add Or Remove Snap-ins** dialog box.
5. Expand **Certificates** (Local Computer), then expand **Personal**, and then expand **Certificates**.
6. Right-click the **Certificates** node, select **All Tasks**, and then select **Request New Certificate**.
7. The **Welcome To The Certificate Import Wizard** page appears. Click **Next**.
8. On the **File To Import** page, type the certificate location.
9. On the **Password** page, type the password provided by the entity that issued this certificate.
10. On the **Certificate Store** page confirm that the location is **Personal**.
11. The **Completing The Certificate Import Wizard** page should appear with a summary of your selections. Review the page and click **Finish**.

Verify that your CA is in the list of trusted root CAs:

1. On each edge server, open an **MMC console**. Click **Start**, and then click **Run**. In the Open box, type **mmc**, and then click **OK**.
2. On the **File** menu, click **Add/Remove Snap-in**, and then click **Add**.
3. In the **Add Standalone Snap-ins** box, click **Certificates**, and then click **Add**.
4. In the **Certificate snap-in** dialog box, click **Computer account**, and then click **Next**.
5. In the **Select Computer** dialog box, ensure that the **Local computer**: (the computer this console is running on) check box is selected, and then click **Finish**.
6. Click **Close**, and then click **OK**. In the console tree, expand **Certificates** (Local Computer), expand **Trusted Root Certification Authorities**, and then click **Certificates**.
7. In the **details** pane, verify that your CA is on the list of trusted CAs. Repeat this procedure on each server.

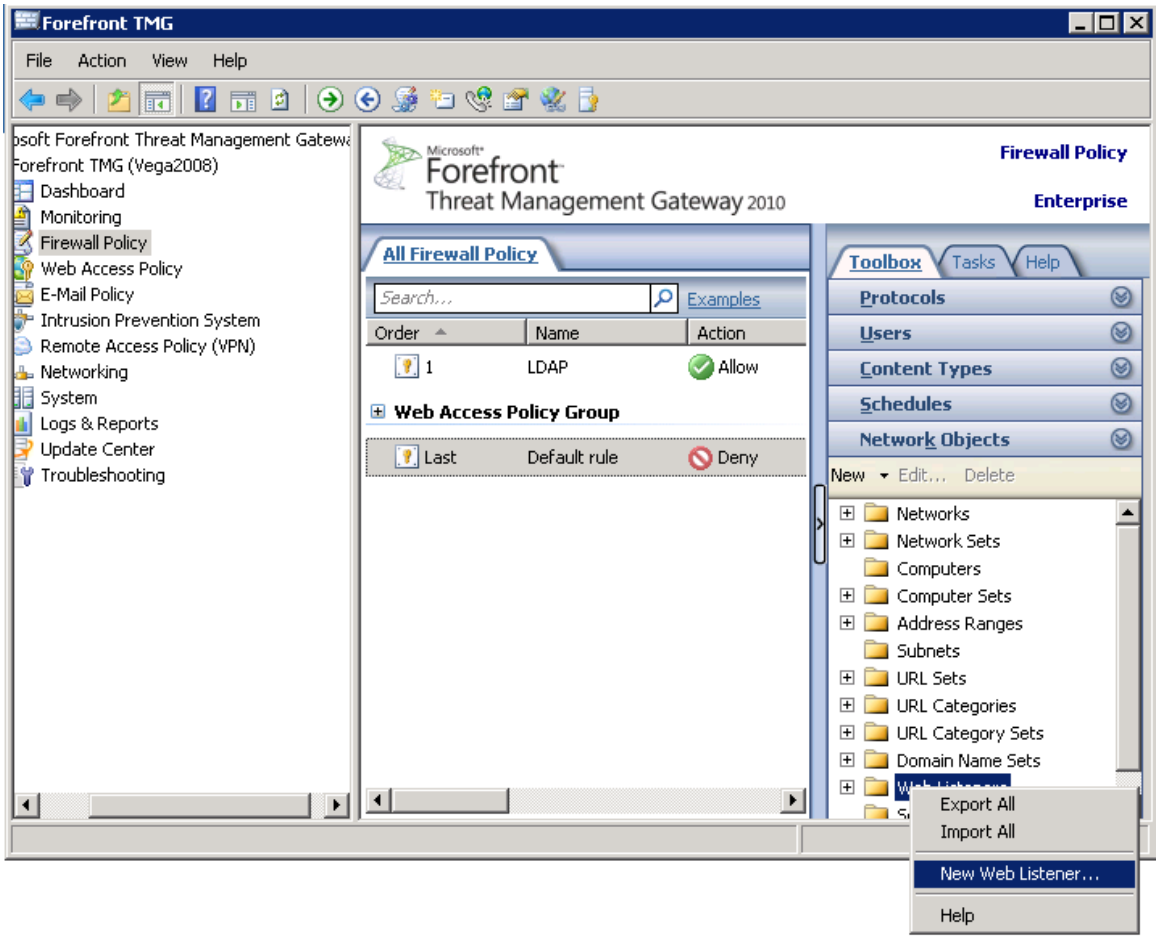
Go to top

Create a New Web Listener for the mobilEcho File Server

1. Open the Forefront TMG Management Console.

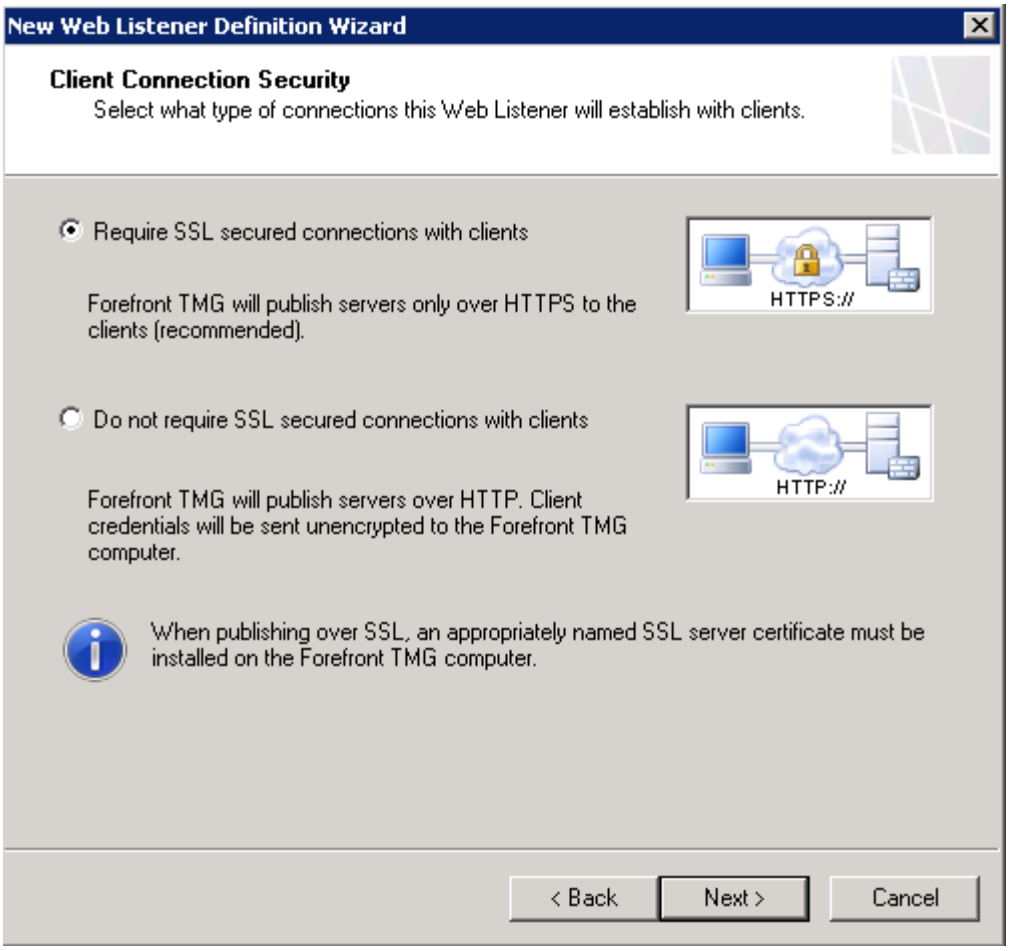
2. Expand Forefront TMG (Array Name or Computer Name) in the left pane and click **Firewall Policy**.

3. In the right pane click the **Toolbox** tab, click **Network Objects**, right-click **Web Listener** and select **New Web Listener** from the menu.

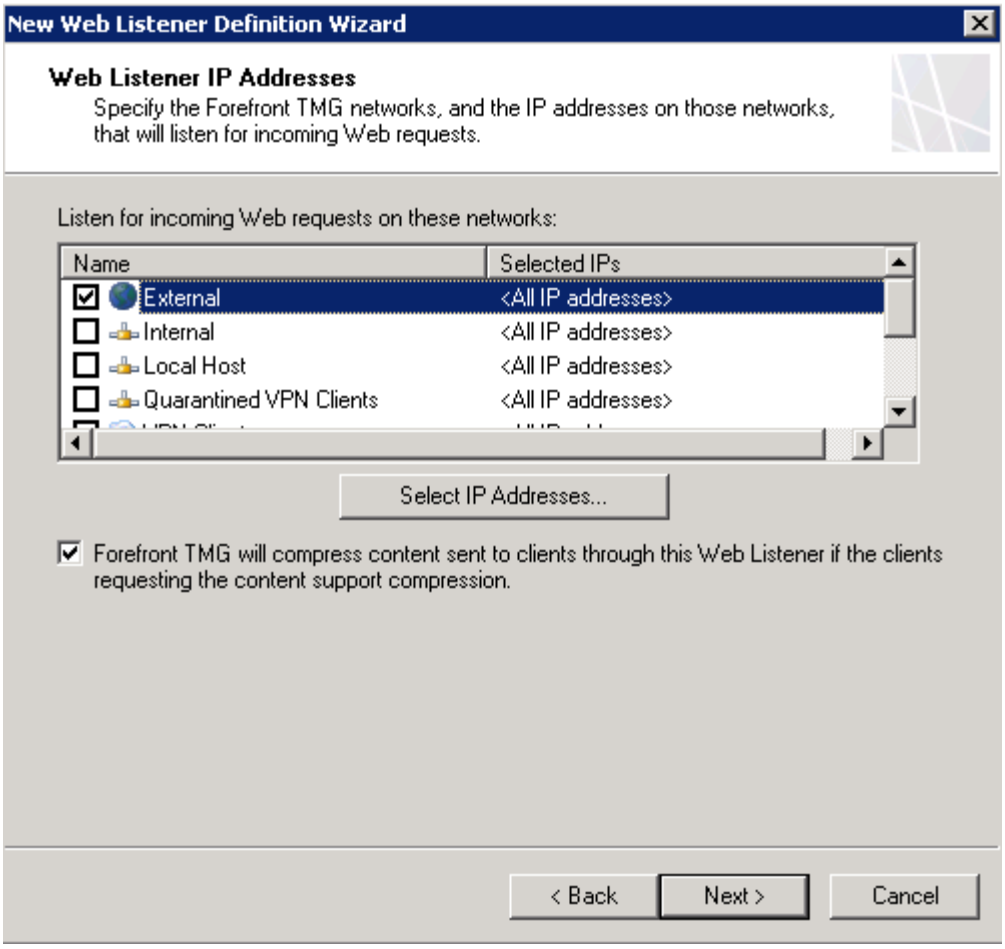


4. The **Welcome to the New Web Listener Wizard** page appears. Give a name to the **Web Listener** (e. g. mobilEcho WL) and click **Next**.

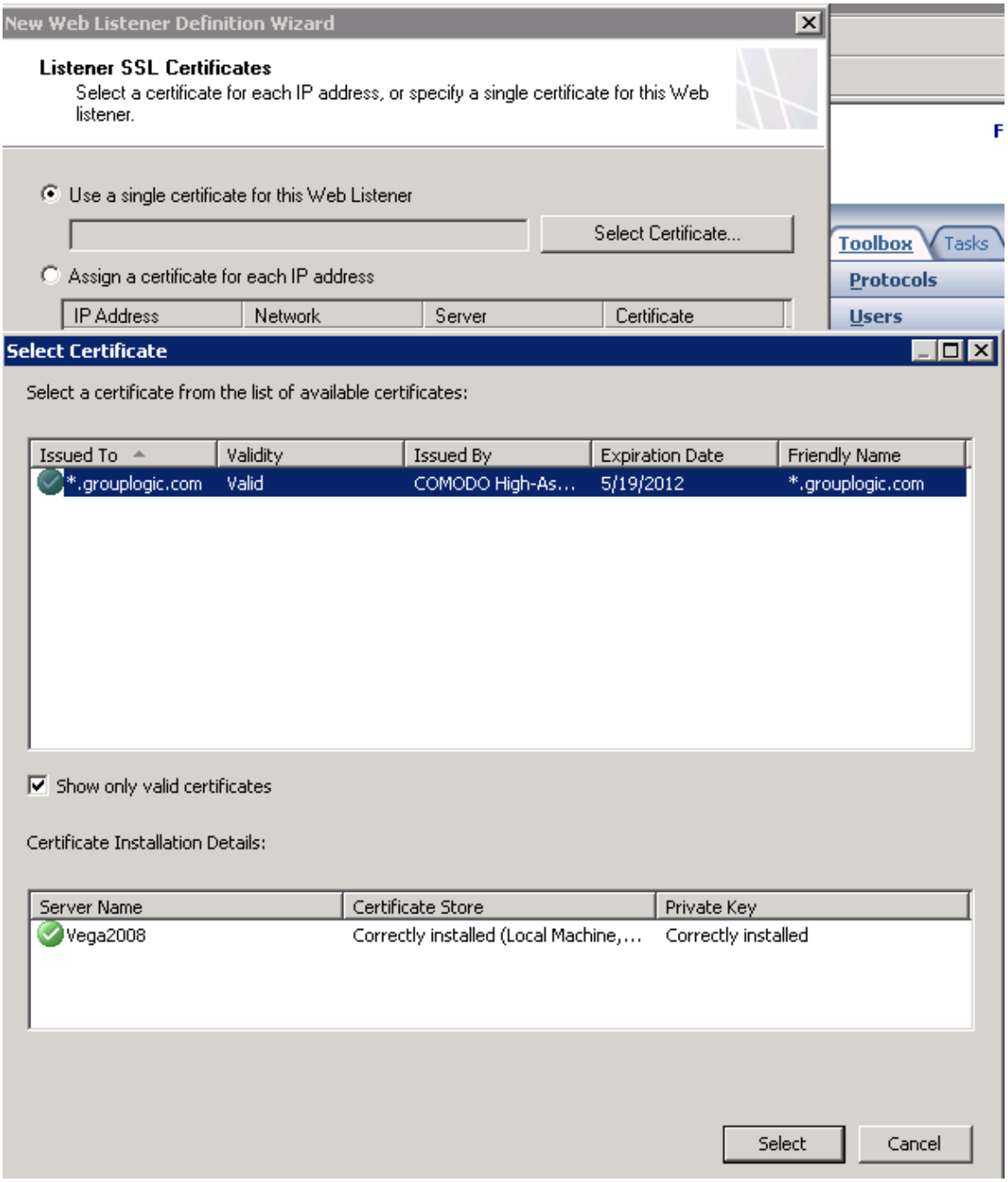
5. On the **Client Connection Security** page select **Require SSL secured connections with clients** and click **Next**.



6. On the **Web Listener IP Addresses** page select **External** and click **Next**.

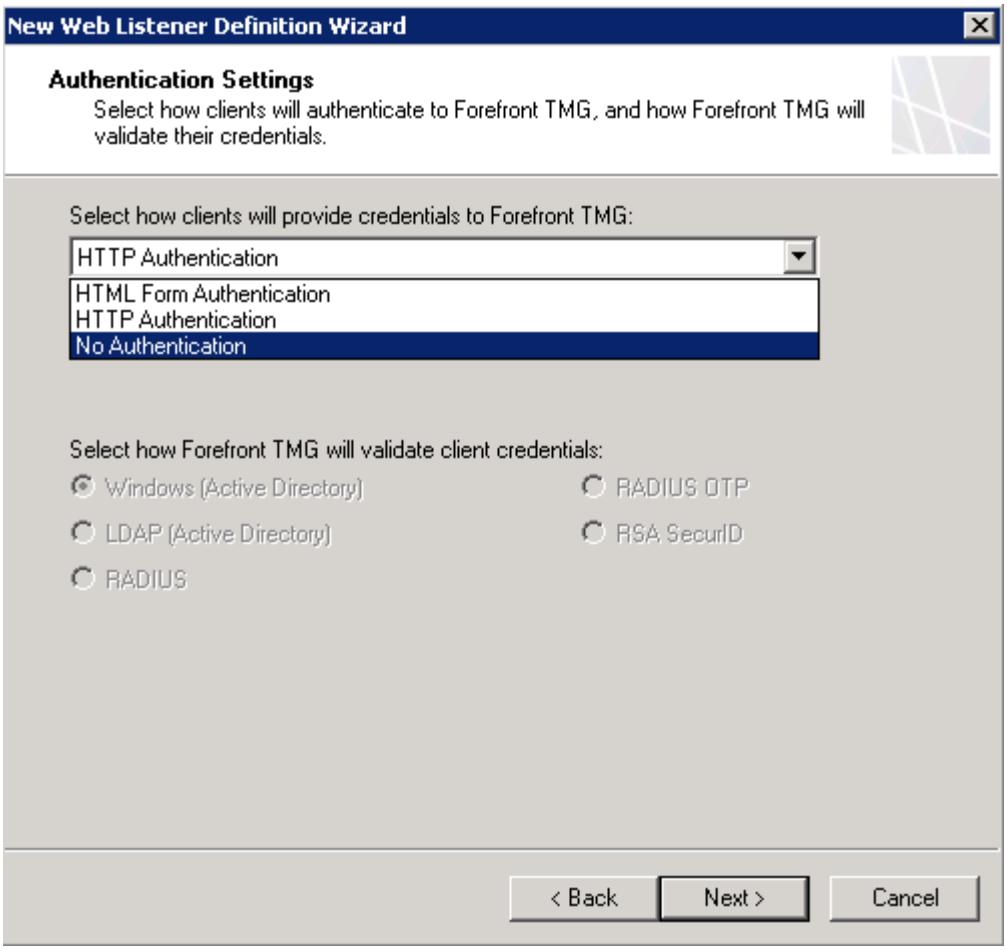


7. On the **Listener SSL Certificates** page select **Use a single certificate for this Web Listener** and click the **Select Certificate** button. Select the appropriate certificate and click the **Select** button to confirm your choice.

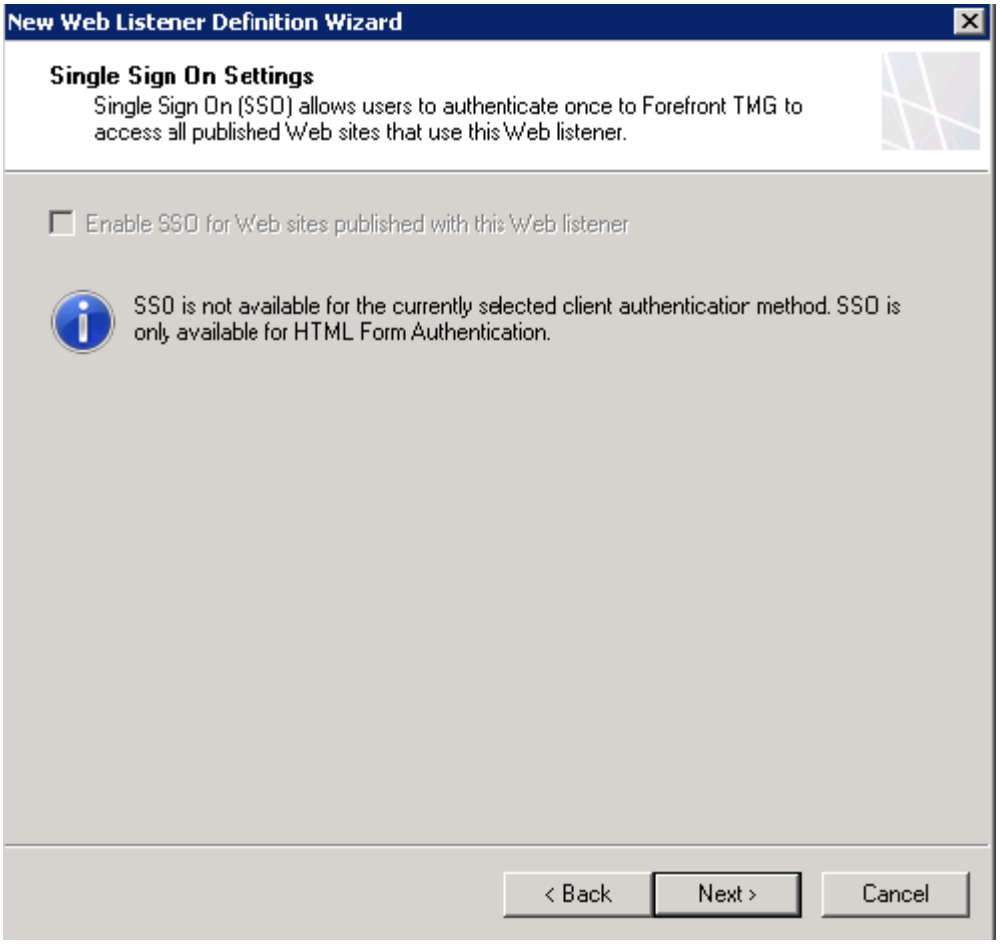


8. Confirm that the correct certificate appears on the **Listener SSL Certificates** page and click **Next**.

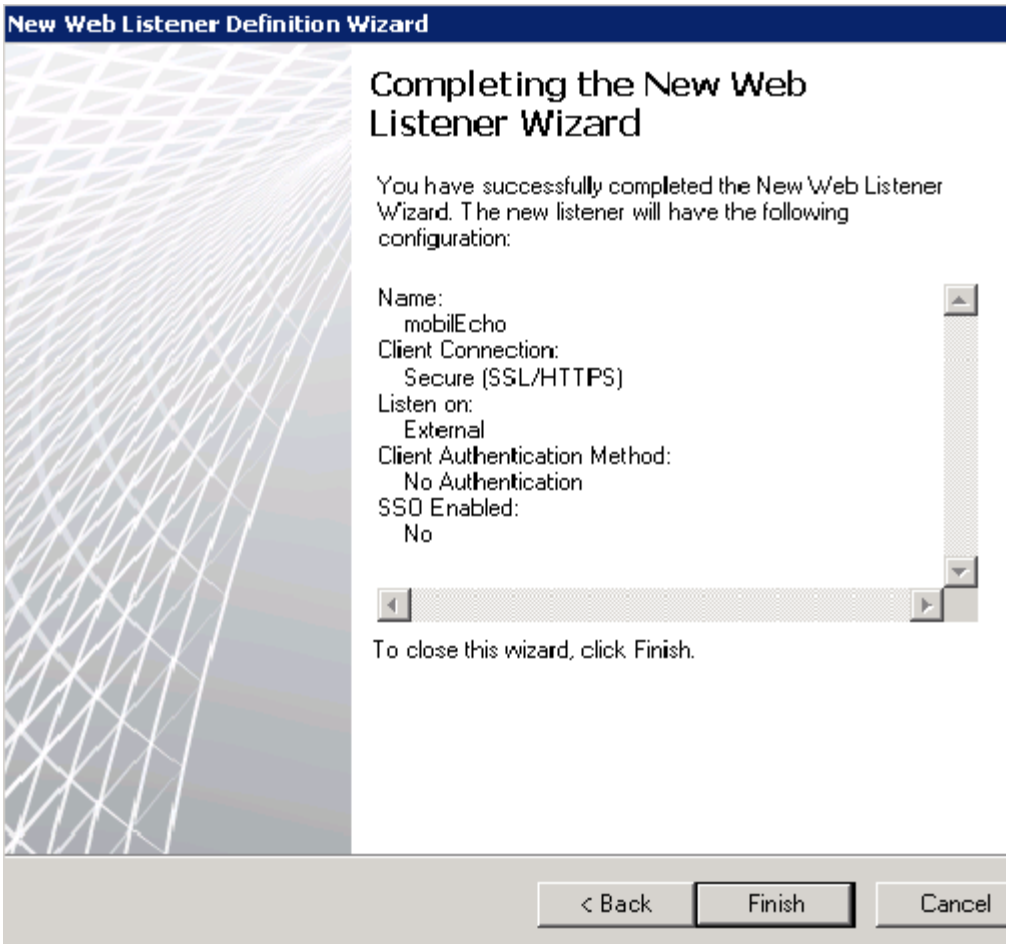
9.On the **Authentication Settings** page choose **No Authentication** from the drop-down menu and click **Next**.



10. On the **Single Sign On Settings** page verify that the **SSO** setting is disabled and click **Next**.



11. Review your selections on the **Completing The New Web Listener Wizard** page and click **Finish**.



12. Click the **Apply** button to commit the changes.

13. In the left pane of the Forefront TMG Management Console click **Monitoring**, then click on the **Confi guration** tab in the middle pane. Keep clicking on the **Refresh Now** link in the right pane (**Tasks** tab) until there is a green icon with the checkbox in front of the TMG computer name (array name).

Go to top

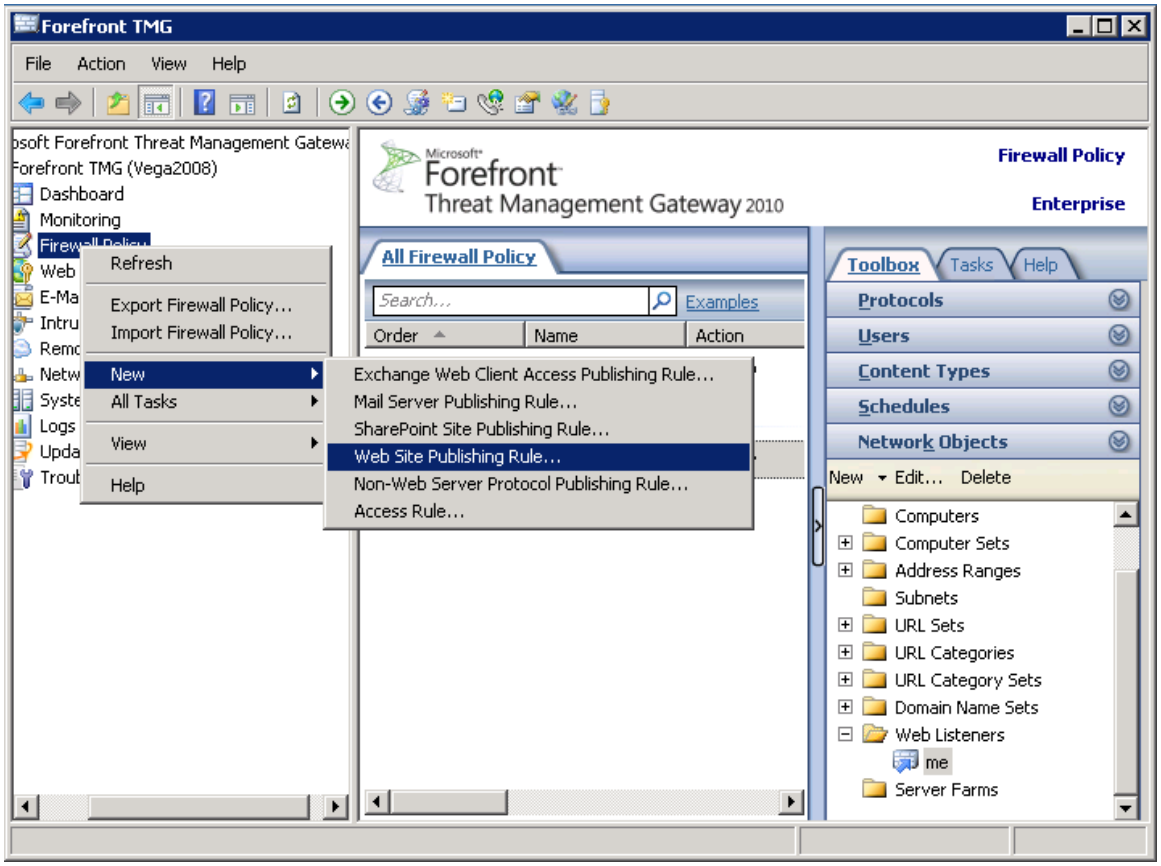
Create a New Web Site Publishing Rule for the mobilEcho File Server

INFO

The steps bellow are tested when the mobilEcho file server's computer is configured to use TMG as a gateway.

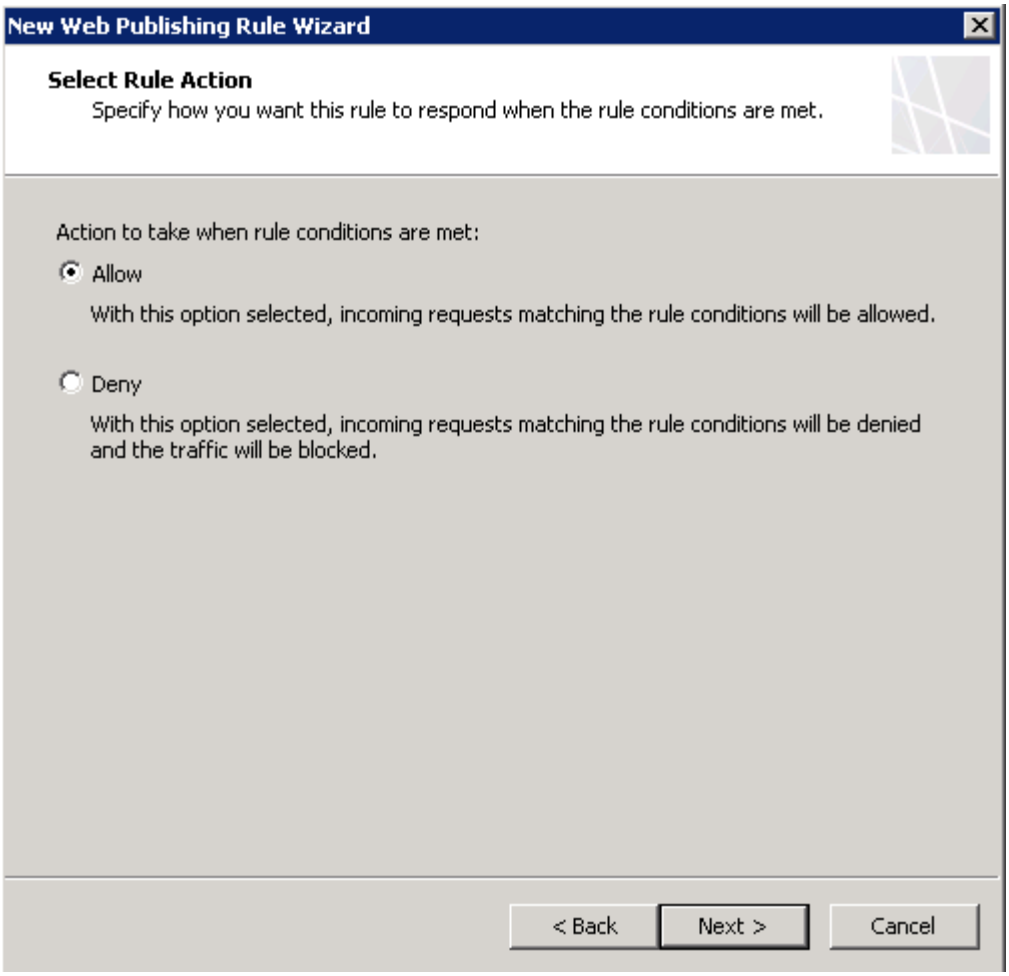
1. In the Forefront TMG Management Console expand Forefront TMG (Array Name or Computer Name) in the left pane.

2. Right-click **Firewall Policy**, select **New**, and click **Web Site Publishing Rule**.

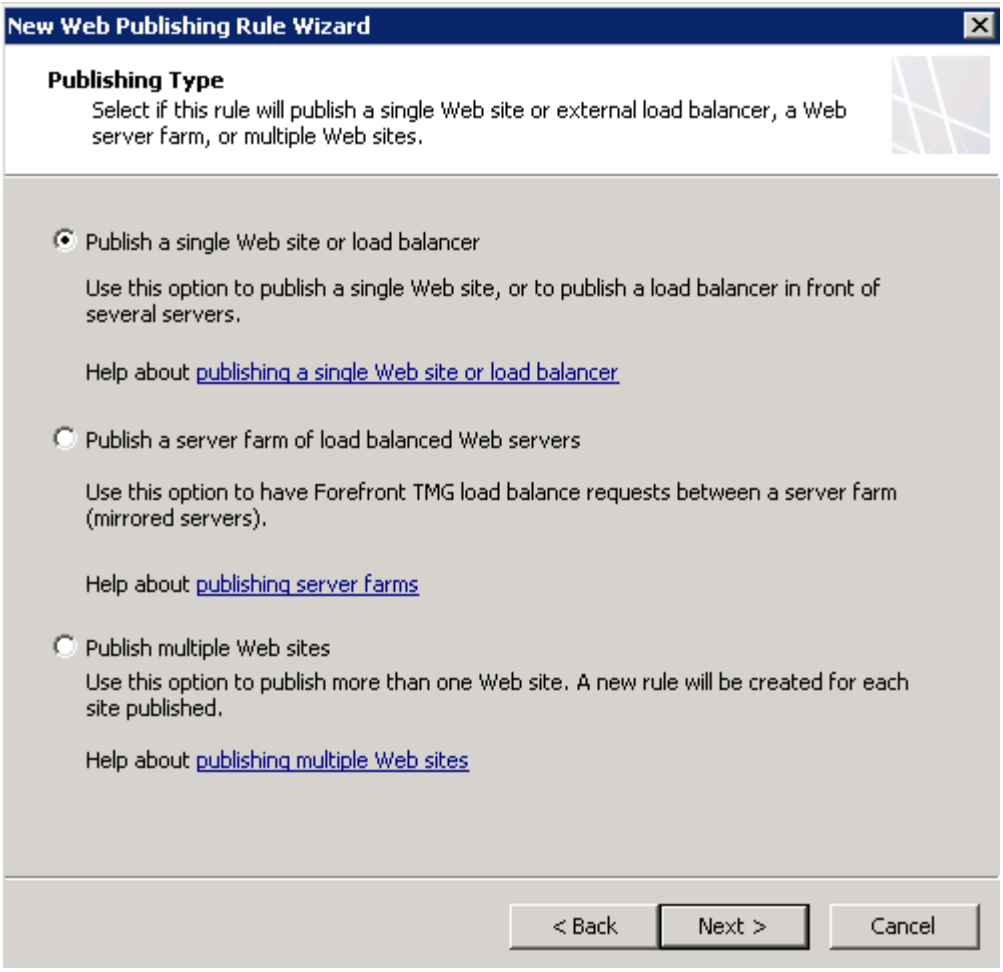


3. The **Welcome to the New Web Publishing Rule Wizard** page appears. Enter a name for the Web publishing rule (e.g. mobilEcho WP) and click **Next**.

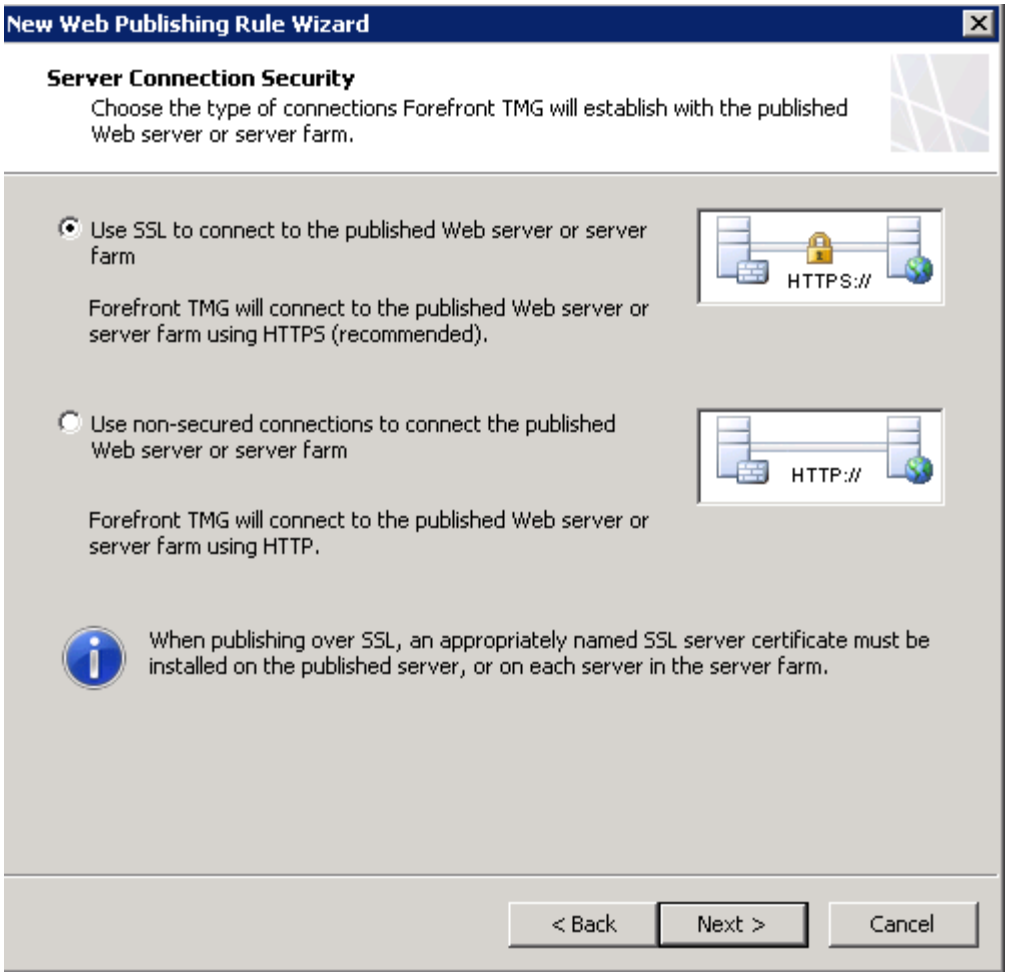
4. On the **Select Rule Action** page verify that the **Allow** option is selected and click **Next**.



5. On the **Publishing Type** page choose the applicable option for your case and click **Next**.

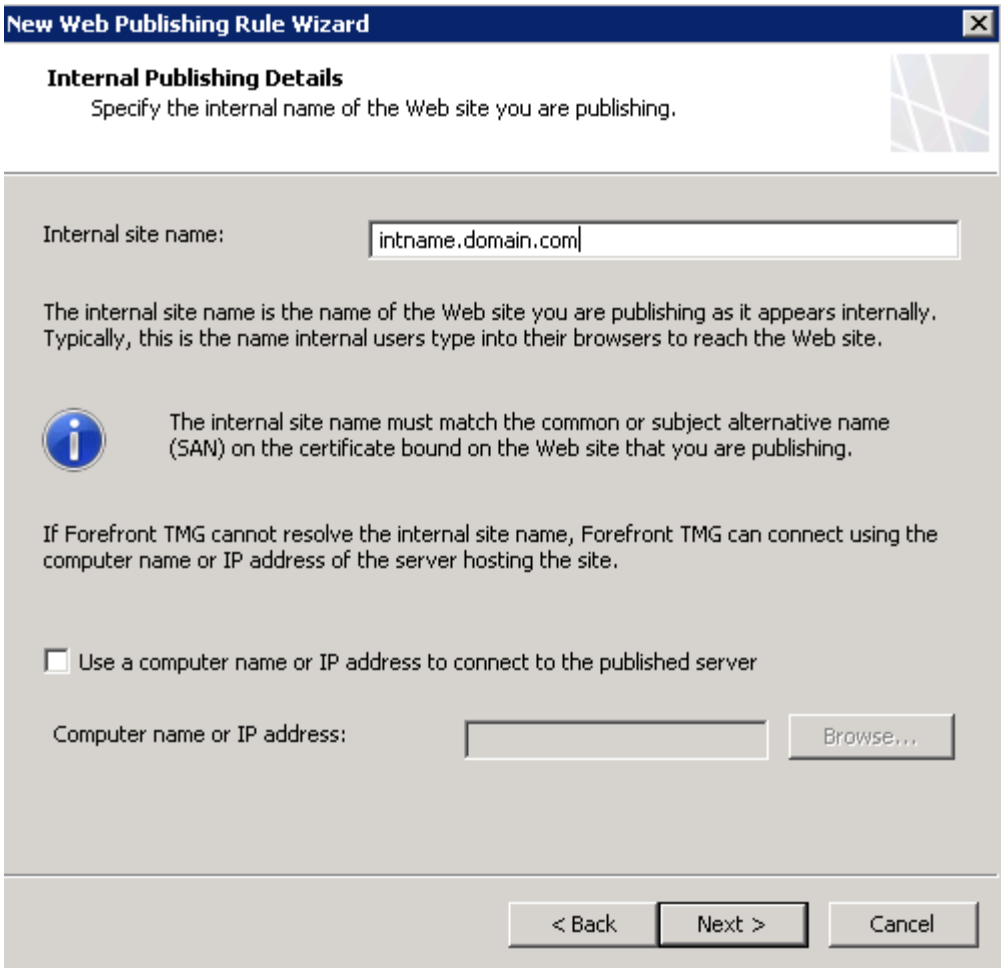


6. On the **Server Connection Security** page choose the **Use SSL to connect to the published Web server or server farm** option and click **Next**.

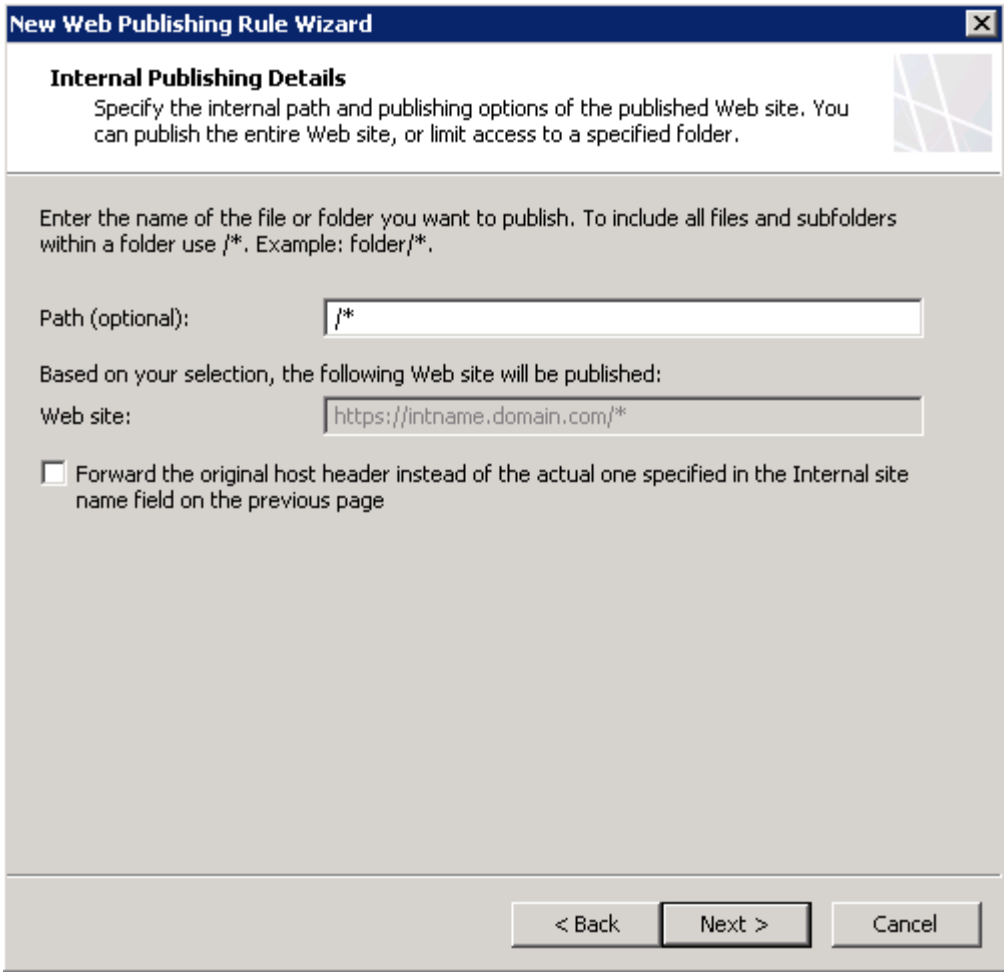


7. On the **Internal Publishing Details** page type "intname.domain.com" in the **Internal site name** field, where **domain** is a placeholder for the domain name the server you want to publish belongs to, and intname is a name you give to this server, which should be different than the external name in order to prevent routing loop. Click **Next** to commit the changes.

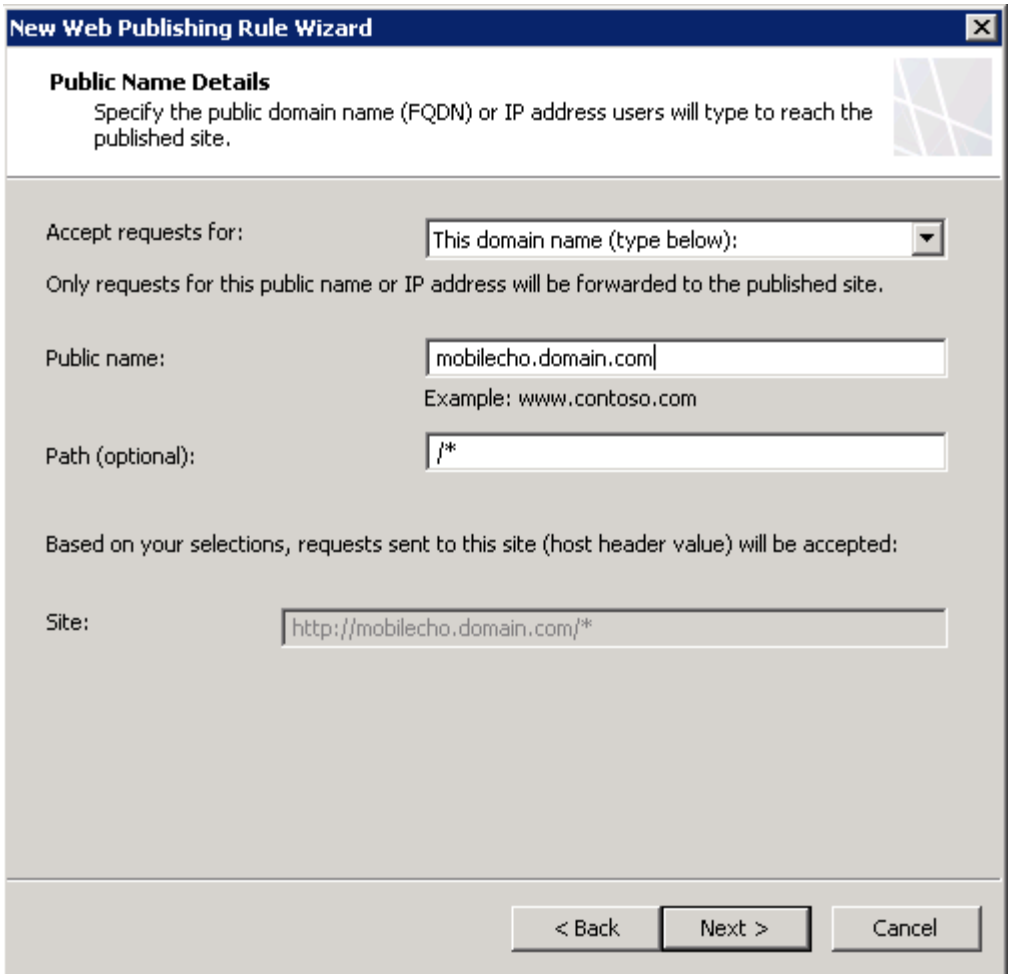
> **NOTE**
>
> Create a DNS entry in the internal DNS server of your organization for "intname.domain.com".



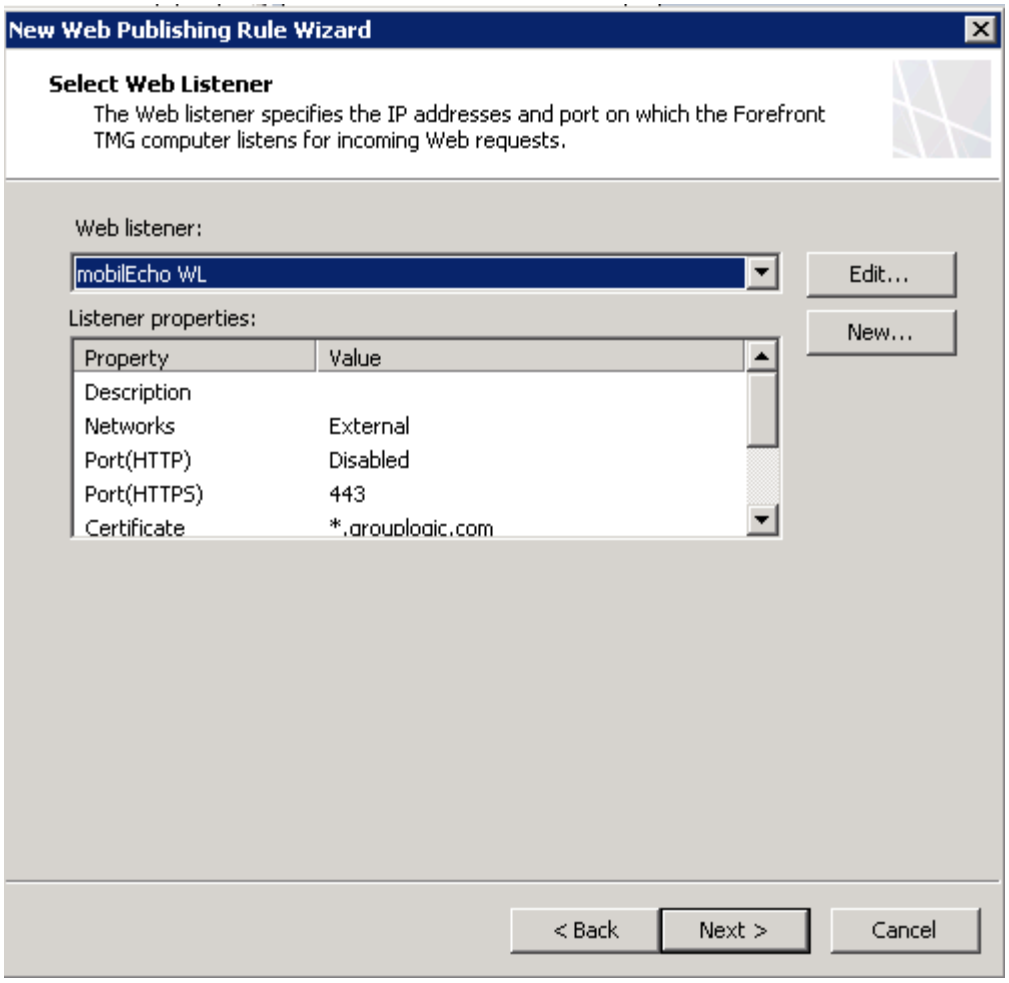
8. On the **Internal Publishing Details** page enter "**/***" in the **Path(optional)** field to allow access to the entire content of the mobilEcho file server. Click **Next**.



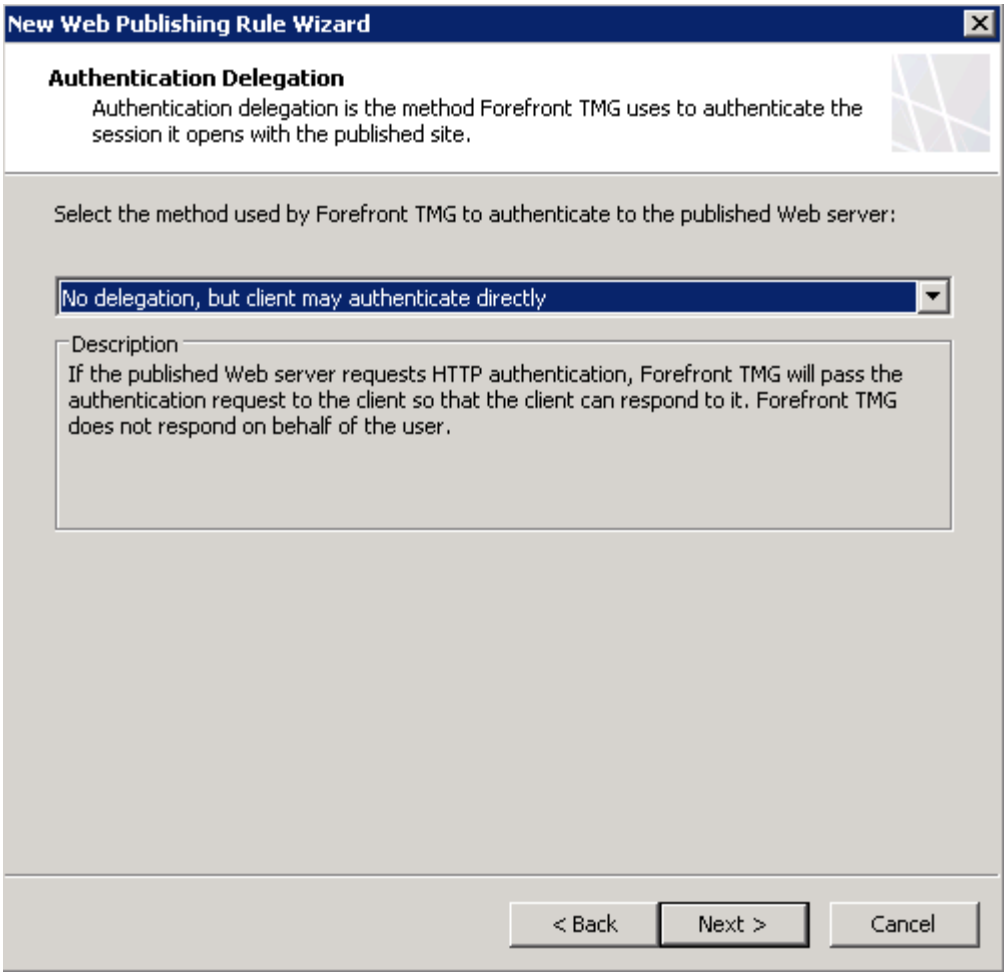
9. On the **Public Name Details** page you need to specify the name that the remote clients will use to connect to the published server. Enter "mobilecho.domain.com" in the **Public name** field, where **domain** i s a placeholder for the domain name of the server you want to publish. Leave the other options the way they are by default and click **Next**.



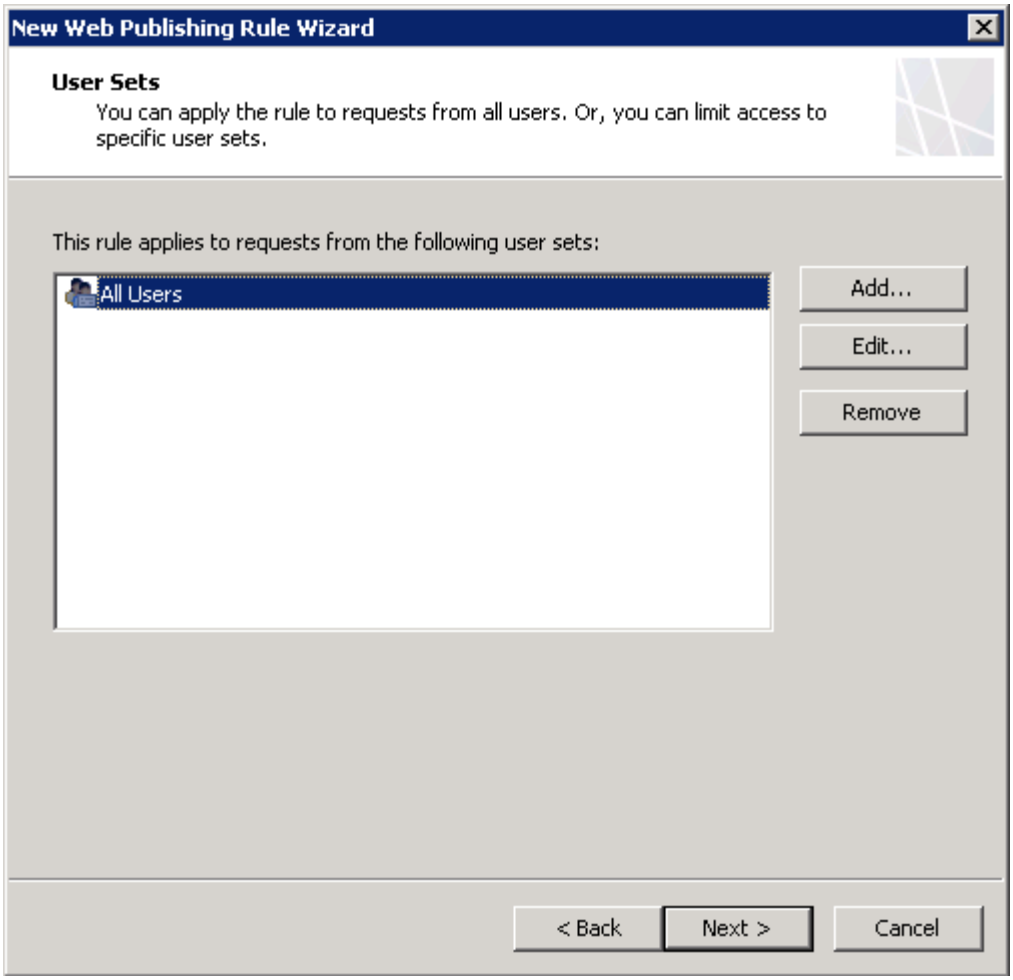
10. On the **Select Web Listener** page select the web listener that you have created for mobilEcho from the drop-down menu and click **Next**.



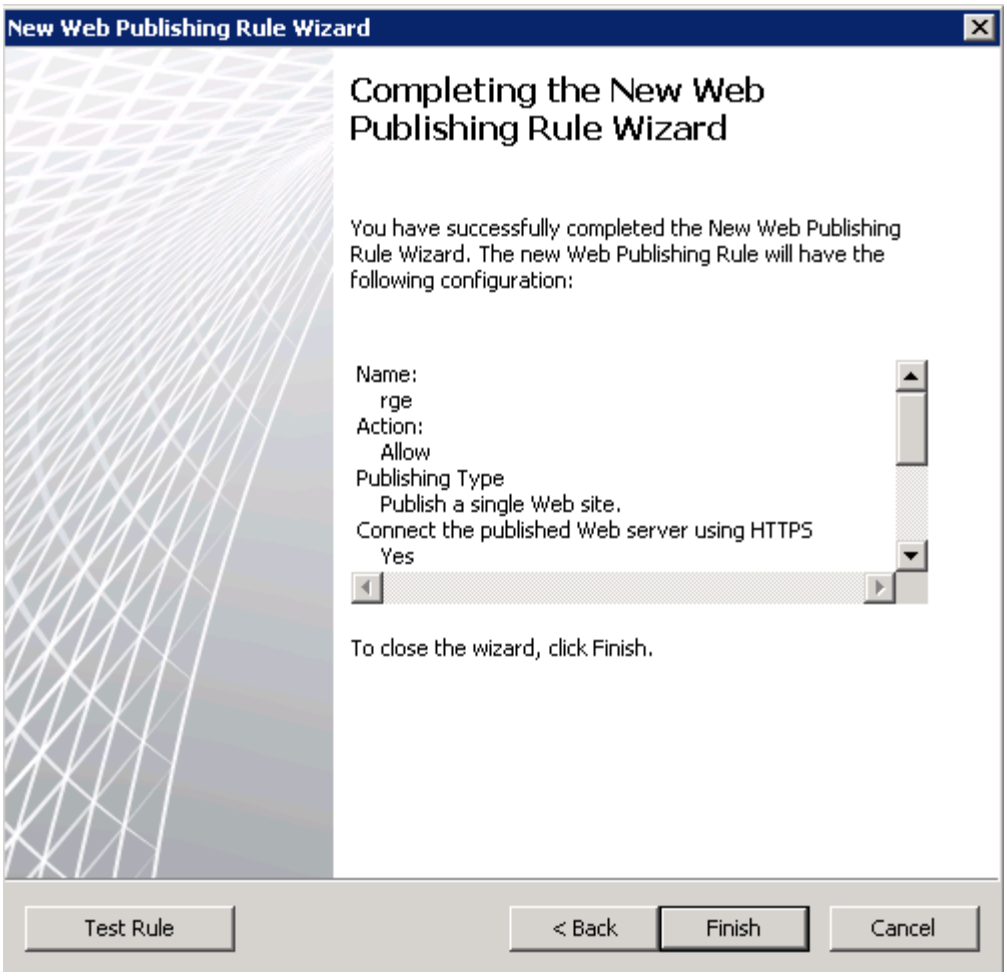
11. On the **Authentication Delegation** page select the **No delegation, but client may authenticate directly** option from the drop-down menu and click **Next**.



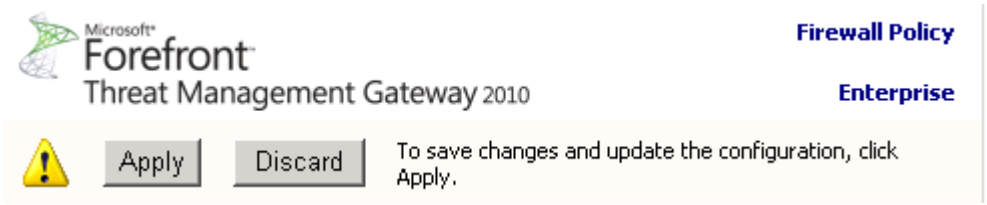
12. On the **User Sets** page verify that the default **All Users** option is present and click **Next** to continue.



13. On the **Completing The New Web Publishing Rule Wizard** page review the summary of your selections. Click **Test Rule** to confirm that the publishing rule is working properly. Click **Finish** to complete the process.



14. Click the **Apply** button to commit the changes.



15. In the left pane of the Forefront TMG Management Console click **Monitoring**, then click on the **Confi guration** tab in the middle pane. Keep clicking on the **Refresh Now** link in the right pane (**Tasks** tab) until there is a green icon with the checkbox in front of the TMG computer name (array name).

Go to top

Configure an External DNS Entry for the mobilEcho File Server

After the TMG configuration process has been completed you need to create a DNS record in the external DNS servers in order to redirect all mobilEcho connections to the external network adapter of TMG. The DNS entry should resolve the name of your mobilEcho file server (mobilecho.domain.com) to the external IP address of the TMG server. All mobilEcho client requests will be sent to and managed by TMG. In this

configuration scenario TMG does not require clients to authenticate, all users will access the mobilEcho file server without any knowledge that the response is coming from the Microsoft Forefront TMG instead.

Go to top

Using mobilEcho with a TMG reverse proxy server.

You can use the mobilEcho Client or the mobilEcho Management Server. This feature is built-in and requires little to no configuration.

In the mobilEcho client app you manually add the server by doing the following:

1. Press the **+** button located in the left corner. This button allows you to add a new server.
2. In the **Server Name or IP Address** field, write the path to your server (e.g. yourserver.companyname.com/mobilecho).
3. Fill in your **credentials** (username / password).
4. Tap **Save.**
5. Done!

For multiple clients you should use the mobilEcho Management Server:

- **Using the reverse proxy server as the management server.**

1. Open the mobilEcho_manager.cfg (located C:\Program Files (x86)\Group Logic\mobilEcho Server\ManagementUI\).
2. Find this line: **MANAGEMENT_SERVER_ADDRESS**
3. Use the path to the server instead of the ip address (e.g. yourserver.companyname.com/mobilecho).
4. **Save** and close the file.

- **Using the reverse proxy server as a provisioned server.**

1. Open the web interface of the management server.
2. Go to the **Servers & Folders** tab.
3. Press **Add New Server.**
4. In the **Server Name or IP Address** field write the path to your server (e.g. yourserver.companyname.com/mobilecho).
5. Enter a **Display name**.
6. Either restrict this server to a couple of users or leave the default setting (available to all users).

Go to top